Ruijie RG-S5315-E Series Switches

S5315_RGOS 12.6(3)B0701P1

Configuration Guide

Document Version: V1.0
Date: July 25, 2025
Copyright © 2025 Ruijie Networks

Copyright

Copyright © 2025 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, no organization or individual is permitted to reproduce, extract, back up, modify, or distribute the content of this document in any manner or form. It is also prohibited to translate the document into other languages or use any or all parts of it for commercial purposes.

and trademarks 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 that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

Personal Data Statement

During the operation or troubleshooting of the products, services, or features you have purchased, certain personal data of users may be collected or used. Therefore, it is essential for you to establish and implement appropriate privacy policies, in compliance with the relevant laws and regulations of the applicable countries or regions, to ensure the complete protection of users' personal data.

If Ruijie Networks is involved in this process, we will strictly adhere to the relevant laws and regulations of the applicable countries or regions and take all necessary actions to safeguard users' personal data.

When discarding, reclaiming, or reusing a device, please ensure to back up or clear any stored data to avoid data leakage. For assistance, please contact our after-sales technical support.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks website: https://www.ruijie.com/
- Online support center: https://www.ruijie.com/support
- Case portal: https://caseportal.ruijie.com
- Community: https://community.ruijienetworks.com
- Email support: service_rj@ruijie.com
- Live chat: https://www.ruijie.com/rita
- Documentation feedback: doc@ruijie.com.cn

Conventions

1. Conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items in square brackets are optional.
[x | y]	Optional items are grouped in braces and separated by vertical bars. One item or no item is selected.
{ x | y }	Optional items are grouped in brackets and separated by vertical bars. One item is selected.
[x | y | ...] *	Optional items are grouped in braces and separated by vertical bars. Several items or no item can be selected.
{ x | y | ... } *	Optional items are grouped in brackets and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
&<1-n>	The parameter before the & sign can be repeated for consecutive 1-n times.

//	A line starting with double slashes is comments.

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 provides configuration information, including models, port types, and command line interfaces, for reference purposes only. In the event of any discrepancy or inconsistency between the manual and the actual version, the actual version shall take precedence.

Basic Configuration

1. Configuring CLI
2. Configuring ZAM
3. Configuring Basic Management
4. Configuring RBAC
5. Configuring Lines
6. Configuring File System
7. Configuring USB
8. Configuring FTP Server
9. Configuring FTP Client
10. Configuring TFTP Server
11. Configuring TFTP Client
12. Configuring HTTP
13. Configuring Syslog
14. Configuring Software Upgrade
15. Configuring Rboot
16. Configuring Uboot
17. Configuring License Management

Contents

1 Configuring CLI 1
1.1 Introduction 1
1.1.1 Accessing the CLI 1
1.1.2 Command Modes 1
1.1.3 System Help 2
1.1.4 Abbreviated Commands 4
1.1.5 No and Default Options of Commands 4
1.1.6 Prompts for Incorrect Commands 4
1.1.7 History Commands 5
1.1.8 Featured Editing 5
1.1.9 Searching and Filtering of the Show Command Output 6
1.1.10 Redirection of the show Command Output 8
1.1.11 Command Alias 8
1.1.12 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 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 "Device")

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.	Device>	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.

Command Mode	Access Method	Prompt	Exit or Entering Next Mode	Function Description of the Mode
Privileged EXEC mode	In User EXEC mode, run the **enable** command to enter privileged EXEC mode.	Device#	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.	Device(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 gigabitethernet 0/1** command to enter interface configuration mode.	Device(config-if-gigabitethernet 0/1)#	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.
Config-vlan (VLAN configuration mode)	In global configuration mode, run the **vlan** *vlan-id* command to enter VLAN configuration mode.	Device(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.

```
Device> ?
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.

```
Device(config)# interface ?
  AggregatePort      Aggregate port interface
  GigabitEthernet    Gigabit Ethernet interface
  Loopback           Loopback interface
  Null               Null interface
  TenGigabitEthernet  10G Ethernet 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:

```
Device(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.

```
Device# d?
debug  delete  dir  disable  disconnect do
```

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

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

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

```
Device(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:

```
Device(config)# int g0/1
Device(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	Backspace key	Delete one character to the left of the cursor.

character.	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.

```
Device# 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
Device# show running-config | regexp include GigabitEthernet [0-9]/1
interface GigabitEthernet 0/1
```

1.1.10 Redirection of the show Command Output

- To redirect the **show** command output to a file, run the following command.

Table 1-8 Redirection of the show Command Output

Command	Description
show any-command > file_path	Redirects the show command output to a file.

To redirect the **show** command output to a file, enter the greater than sign (>) and add the file name (Flash, Tmp, and USB partitions are supported) following this sign.

```
Device# show running-config > flash:output.txt
```

1.1.11 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.

```
Device(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.

```
Device# 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.

```
Device# 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.

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

- Caution

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

1.1.12 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 1-9 Monitoring of the CLI

Command	Purpose
show aliases [*mode*]	Displays all command aliases or the command aliases in specific command mode.
show cli session	Displays information about running CLI sessions.
show cli model state	Displays the CLI service module readiness status.

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

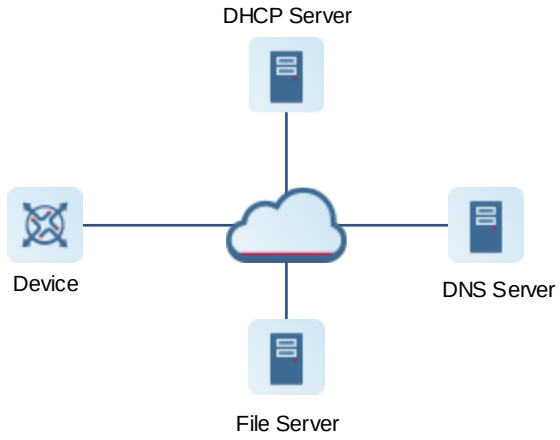
1.1 Introduction

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

Based on the file name of the Python script and the IP address of the ZAM server (on which the TFTP server function will be deployed) obtained during DHCP, the device downloads the corresponding configuration script from the ZAM server.

Upon downloading above, the device executes the configuration script and downloads the corresponding configuration file or version from the ZAM 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 ZAM 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
```

- Deploy the TFTP server function on the ZAM server. Store the Python script file in the root directory of the ZAM 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 ZAM 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
debug zam	Enables the ZAM framework event debugging.
show zam	Displays the current configurations and status of ZAM.
show amaint-app loop-detect	Display loop information.
show amaint-app neighbor	Displays neighbor information detected by the device.

1.5 Configuration Examples

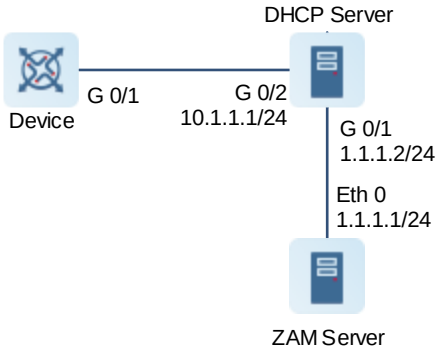
1.5.1 Configuring ZAM

1. Requirements

Manage and control onboarding and deployment of all devices in the network in a unified manner. Realize the unified management of onboarding and deployment of all devices.

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
```

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
```

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.

```
*May 13 15:47:36: %ZAM-6-EVENT: Get tftp server ip 1.1.1.1.
*May 13 15:47:36: %IPMIX-6-ADDRESS_ASSIGN: Interface VLAN 1 assigned DHCP address
10.1.1.2, mask 255.255.255.0.
*May 13 15:47:36: %ZAM-6-EVENT: Get boot file name zam.py.
*May 13 15:47:42: %ZAM-6-EVENT: Download script success, rename to zam.py.
*May 13 15:47:42: %ZAM-6-INFO: Begin to exec script zam.py.
Thu May 13 15:47:46 2021 INFO: script(version:1.0.12440) running...
Thu May 13 15:47:46 2021 DEBUG: server ip: 1.1.1.1, port type: SVI
Thu May 13 15:47:46 2021 DEBUG: current version: S5700H_RGOS12.x(master)
Thu May 13 15:47:46 2021 DEBUG: current patch: NA
```

```
Thu May 13 15:47:47 2021 DEBUG: execute upload command: copy
flash:/G1NQ7UW700483.POAP tftp://1.1.1.1/POAP_STARTUP/G1NQ7UW700483.POAP...
Thu May 13 15:47:47 2021 DEBUG: upload G1NQ7UW700483.POAP success
Thu May 13 15:47:47 2021 DEBUG: begin to download G1NQ7UW700483.params ...
Thu May 13 15:47:47 2021 DEBUG: execute download command: copy
tftp://1.1.1.1/POAP_CFG/G1NQ7UW700483.params flash:/poap.tmp.params...
Thu May 13 15:47:48 2021 DEBUG: download G1NQ7UW700483.params success
Thu May 13 15:47:48 2021 DEBUG: parse image_name=57H_5PL4_0329.bin
Thu May 13 15:47:48 2021 DEBUG: begin to download G1NQ7UW700483.cfg ...
Thu May 13 15:47:48 2021 DEBUG: execute download command: copy
tftp://1.1.1.1/POAP_CFG/G1NQ7UW700483.cfg flash:/poap.tmp.cfg...
Thu May 13 15:47:48 2021 DEBUG: download G1NQ7UW700483.cfg success
Thu May 13 15:47:48 2021 INFO: download G1NQ7UW700483.cfg success, save to
flash:/poap.tmp.cfg
Thu May 13 15:47:48 2021 INFO: begin to download 57H_5PL4_0329.bin ...
Thu May 13 15:47:48 2021 DEBUG: execute download command: copy
tftp://1.1.1.1/POAP_IMAGE/57H_5PL4_0329.bin tmp:/poap.image.bin...
Thu May 13 15:54:20 2021 DEBUG: download 57H_5PL4_0329.bin success
Thu May 13 15:54:20 2021 INFO: download 57H_5PL4_0329.bin success, save to
tmp:/poap.image.bin
Thu May 13 15:54:20 2021 INFO: upgrade system begin...
< The terminal is lock >
Upgrade start
!!!!100%
Upgrade skip, reason: The version in device is the same
< The terminal is unlock >
Thu May 13 15:54:43 2021 INFO: upgrade status: skip
Thu May 13 15:54:53 2021 DEBUG: rename file poap.tmp.cfg to config.text
Thu May 13 15:54:53 2021 INFO: script ending...
Thu May 13 15:54:54 2021 DEBUG: execute upload command: copy flash:/poap.tmp.log
tftp://1.1.1.1/POAP_LOG/G1NQ7UW700483.LOG...
Thu May 13 15:54:55 2021 DEBUG: upload G1NQ7UW700483.LOG success
Thu May 13 15:54:56 2021 DEBUG: execute upload command: copy flash:/G1NQ7UW700483.ok
tftp://1.1.1.1/POAP_STATUS/G1NQ7UW700483.ok...
Thu May 13 15:54:56 2021 DEBUG: upload G1NQ7UW700483.ok success
*May 13 15:55:00: %ZAM-6-EVENT: Script exec success, request device reset now.
*May 13 15:55:00: %DP-3-RESET_DEV: Reset device 1 due to zam reload device.
*May 13 15:55:02: %ZAM-6-EVENT: Script exec success, request device reset now.
*May 13 15:55:02: %DP-3-MACHINE_RESTART: MACHINE_RESTART.
```

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 do shell exec
Server ip           :1.1.1.1
Usb path            :NULL
Interface name       :VLAN 1
Interface type       :SVI
Succ Interface name   :VLAN 1
Script URL          :tftp://1.1.1.1/zam.py
```

6. Configuration Files

- DHCP server configuration file

```
hostname Dhcp_Server
!
ip dhcp pool zam
 option 66 ascii 1.1.1.1
 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 Protocol Specification 2

1.4 Restrictions and Guidelines 2

1.5 Configuration Task Summary 2

1.6 Configuring Basic System Parameters 3

1.6.1 Configuration Tasks 3

1.6.2 Configuring Connection to the Supervisor Module or Member Device 3

1.6.3 Configuring a System Name and Command Prompt 4

1.6.4 Configuring System Notifications 4

1.6.5 Configuring the System Clock 6

1.7 Enabling or Disabling a Specific Service 7

1.8 Configuring Passwords and Privilege Levels 7

1.9 Configuring Telnet Login 10

1.9.1 Configuration Tasks 10

1.9.2 Configuring the Telnet Service 10

1.9.3 Configuring Telnet Access Security 12

1.10 When AAA is enabled, non-AAA authentication is disabled by default.Configuring Logging in to Other Devices through Telnet 14

1.10.1 Overview 14

1.10.2 Restrictions and Guidelines 14

1.10.3 Procedure 15
1.11 Configuring Management 15
1.11.1 Configuration Tasks 15
1.11.2 Running Batch File Commands 15
1.11.3 Configuring Multiple-configuration Booting 16
1.11.4 Configuring Automatic Configuration File Backup to a Remote Server 16
1.11.5 Rolling Back System Configurations 17
1.11.6 Saving the Configuration 19
1.11.7 Configuring the Login Failure Recording Function 19
1.12 Configuring a Restart Policy 19
1.12.1 Configuration Tasks 19
1.12.2 Configuring Immediate Restart 19
1.12.3 Configuring Scheduled Restart 20
1.13 Configuring a Memory Usage Threshold 21
1.13.1 Overview 21
1.13.2 Procedure 21
1.14 Configuring a CPU Usage Threshold 21
1.14.1 Overview 21
1.14.2 Restrictions and Guidelines 21
1.14.3 Procedure 21
1.15 Configuring System Version Monitoring 22
1.15.1 Overview 22
1.15.2 Procedure 22
1.16 Monitoring and Maintenance 22

1.17 Configuration Examples.....24

1.17.1 Configuring Login Authentication and Telnet Service.....24

1.17.2 Configuring Basic System Parameters.....25

1 Configuring Basic Management

1.1 Overview

To reduce the inconvenience caused by on-site maintenance, IT devices are widely managed remotely. Even initial deployment can be carried out remotely. Remote management needs to consider the various operational needs of network administrators and the security of device management. A series of functions of basic management address security, maintenance and monitoring issues.

- Security: Basic management provides permissions, encryption authentication and access control to ensure device security.
- Maintenance: Basic management provides flexible configuration management methods, such as backup, rollback and batch execution, etc.
- Monitoring: Basic management provides various software and hardware monitoring functions to display information of memory, CPU, bus, session, etc..

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*.
RADIUS	The Remote Authentication Dial in User Service (RADIUS) is the most widely used AAA protocol.

Concept	**Description**
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.
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 Protocol Specification

RFC 874: Telnet Protocol Specification

1.4 Restrictions and Guidelines

- Pay attention to the following when entering a string:
  - If the string is in double quotation marks, any characters can be inside the quotation marks. To include quotation marks in the string, you must translate the character prefix. For example, if the input string is "hello my friend \"Haha\"", the saved string is as follows: hello my friend "Haha".
  - If the string does not contain a right quotation mark, the string ends at the end of the command line. For example, if the string is “hello my friend \"Haha\", the string is saved as follows: hello my friend "Haha".
  - A string without quotation marks cannot carry delimiters, such as spaces and tabs. The valid value is a string of ha-ha or Haha.

1.5 Configuration Task Summary

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

Basic functions:

- Configuring Basic System Parameters
  - Configuring Connection to the Supervisor Module or Member Device
  - Configuring a System Name and Command Prompt
  - Configuring System Notifications
  - Configuring the System Clock
- Enabling or Disabling a Specific Service

Permission and login control:

- Configuring Passwords and Privilege Levels
- Configuring Telnet Login
  - Configuring the Telnet Service
  - Configuring Telnet Access Security
  - Configuring Logging in to Other Devices through Telnet

Configuration and maintenance:

- Configuring Management
  - Running Batch File Commands
  - Configuring Multiple-configuration Booting
  - Configuring Automatic Configuration File Backup to a Remote Server
  - Rolling Back System Configurations
  - Saving the Configuration
- Configuring a Restart Policy
  - Configuring Immediate Restart
  - Configuring Scheduled Restart

1.6 Configuring Basic System Parameters

1.6.1 Configuration Tasks

Basic system parameter configuration includes the following tasks:

- Configuring Connection to the Supervisor Module or Member Device
- Configuring the System Clock
- Configuring a System Name and Command Prompt
- Configuring System Notifications

1.6.2 Configuring Connection to the Supervisor Module or Member Device

1. Overview

By configuring this function, the administrator can connect to the supervisor module or member device in the VSU active-standby (chassis device) environment.

This function allows an administrator to connect to a member device in a VSU environment that involves multi-device stacking.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Connect to the supervisor module or member device.

(Standalone mode)

session master

(VSU mode))

session { **device** *device-number* | **master** }

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 system name is **Ruijie**.

(4) Configure a command prompt.

prompt *prompt-string*

(5) 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. The text length must not exceed

- 2047 bytes.
- 1023 bytes.
- 255 bytes.

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.

1.6.5 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.
- If daylight saving time and time zone need to be configured at the same time, configure them by running commands in the following order: **clock timezone** and then **clock summer-time**. Otherwise, the daylight saving time configuration exists but does not take effect.
- If both daylight saving time and time zone configurations exist on the device, when you run the **no clock timezone** command to delete the time zone configuration, the daylight saving time configuration is also deleted. In this case, you need to reconfigure the daylight saving time.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure the system date and clock.

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

The default system clock is 1970-01-01 00:00:00.

(3) (Optional) Update the hardware clock.

clock update-calendar

The system is not configured to synchronize the hardware time with the software time by default.

(4) (Optional) Configure the hardware clock of the device

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

The default hardware time of the device is 1970-01-01 00:00:00.

(5) (Optional) Configure the system to synchronize the software time with the hardware time.

clock read-calendar

The system is not configured to synchronize the software time with the hardware time by default.

(6) Enter the global configuration mode.

configure terminal

(7) (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*]]

The summer time is not configured by default.

(8) (Optional) Configure the time zone.

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

The time zone is set as Universal Time Coordinated (UTC) by default.

1.7 Enabling or Disabling a Specific Service

1. Overview

When the system is running, you can dynamically adjust system services, including 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 { **snmp**-**agent** | **ssh**-**server** | **telnet**-**server** | **web**-**server** [**http** | **https** | **all**] }

The Simple Network Management Protocol (SNMP) agent, Secure Shell (SSH) server, Telnet server, and Web server are disabled by default.

1.8 Configuring Passwords and Privilege Levels

1. Overview

Privilege levels and passwords for different privilege levels can be configured to distinguish access needs of different users' 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** or **disable** command to raise or lower 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.

3. Procedure

(1) Enter user EXEC mode.

(2) Change the user privilege level.

- Increase the privilege level.

  enable [*privilege-level e*]

  When the RBAC function is enabled, you can run this command to switch the role of the current terminal. By default, the role is switched to network-admin.

- Lower the privilege level.

  disable [*privilege-level*]

  The privilege level specified in this command must be lower than the current level.

  When the RBAC function is enabled, this command is unavailable.

(3) Enter the privileged EXEC mode.

enable

(4) (Optional) Display help information.

help

(5) Change the privilege level.

- 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.

- Lower the privilege level.

  disable [*privilege-level*]

  The privilege level specified in this command must be lower than the current level.

  When the RBAC function is enabled, this command is unavailable.

(6) Enter the global configuration mode.

configure terminal

(7) Configure a password.

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

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

(8) Configure a secret.

enable secret { [**level** *secret-level*] | [**role** *role-name*] } { [**0**] *password* | { **5** | **8** } *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.

(9) (Optional) Configure a handling policy when the number of consecutive authentication failures to enter the privileged EXEC mode reaches the limit.

enable user-block { **disable** | **failed-times** *times* **period** *period* | **reactive** *time* }

The allowed maximum number of consecutive authentication failures is 3, the period for resetting the consecutive authentication failure count is 10 minutes, and a user will be locked for 10 minutes after the number of consecutive authentication failures reaches the limit. You can run the **enable user-block disable** command to disable the function.

(10) (Optional) Configure the algorithm used for encryption.

enable algorithm-type { **md5** | **sha256** }

The SHA-256 algorithm is used for encryption by default.

(11) (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.

(12) (Optional) Enable level increase logging.

login privilege log

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

(13) Configure command privilege levels.

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

(14) Enter the line configuration mode.

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

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

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

(16) 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.

(17) Exit the configuration mode and return to the upper-level mode or exit the command line interface (CLI) from the privileged EXEC mode.

exit

1.9 Configuring Telnet Login

1.9.1 Configuration Tasks

Telnet login includes the following tasks, which are all optional and can be chosen according to the actual situation:

- Configuring Telnet Service
- Configuring Telnet Access Security
- Configuring Logging in to Other Devices through Telnet
- Saving the Configuration
- Configuring the Login Failure Recording Function

1.9.2 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

Telnet allows you to use IPv4 and IPv6 addresses for communication. The telnet server can accept connection requests sent from a telnet host with an IPv4 or IPv6 address. The telnet client can initiate connection requests to a host configured with an IPv4 or IPv6 address.

When the telnet server service is enabled on the device, you can use the telnet client to connect to the device securely 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, 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.
- With the IP address blocking function enabled, 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 be used to 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 the listening port of the Telnet server.

ip telnet-server port *port-number*

The default port number is 23.

(4) Configure an ACL for the telnet server.

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

No IPv4 ACL filtering rule is configured by default.

ipv6 telnet access-class *ipv6-acl-name*

No IPv6 ACL filtering rule is configured by default.

(5) 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.

(6) 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.

(7) 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.

(8) Enter the line configuration mode.

line vty *line-number*

(9) (Optional) Configure the connection timeout time.

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

The default connection timeout time of the device on a line is 10 minutes.

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

(10) (Optional) 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.

(11) (Optional) Enable EXEC prompt information display for a specific line.

exec-banner

EXEC prompt information display is enabled for all lines by default.

(12) (Optional) Enable MOTD prompt information display for a specific line.

motd-banner

MOTD prompt information display is enabled for all lines by default.

1.9.3 Configuring Telnet Access Security

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* [**algorithm-type** { **md5** | **sha256** }] [**login mode** { **console** | **ssh** | **telnet** | **ftp** }] [**online amount** *amount-number*] [**permission** *oper-mode path*] { [**privilege** *privilege-level*] | [**role** *text-string*] } [**reject remote-login**] [**vid** *vid-number*] [**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 *file-name*

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

username export *file-name*

(6) Enter the line configuration mode.

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

(7) Configure the encryption type for line-based login.

algorithm-type { **md5** | **sha256** }

The default encryption type for line-based login is SHA256.

(8) Configure an MD5/SHA-256 irreversible encrypted password for line-based login.

secret { [**0**] *password* | { **5** | **8** } *encrypted-secret* }

No encrypted password is configured for line-based login by default.

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

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

No password is configured for line-based login by default.

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

login local

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

(11) (Optional) Configure AAA authentication for line-based login.

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

When AAA is enabled, the **default** authentication method is used by default.

(12) (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.

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

a Return to the global configuration mode.

exit

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

login access non-aaa

1.10 When AAA is enabled, non-AAA authentication is disabled by default.Configuring Logging in to Other Devices through Telnet

1.10.1 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.

1.10.2 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.
  - Before you remotely log in to the device through Telnet, you can run the **enable service telnet-server** command to enable the Telnet server service on the device.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

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

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

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

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

1–99

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

disconnect *session-id*

(5) (Optional) Specify the IP address of an interface as the source IP address of a Telnet connection. .

ip telnet source-interface *interface-type interface-number*

The Telnet source interface is the reachable outbound interface of the Telnet server by default.

(6) (Optional) Return to the privileged EXEC mode.

end

(7) (Optional) Lock the current terminal connected to a line.

lock

1.11 Configuring Management

1.11.1 Configuration Tasks

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

- **Running Batch File Commands**
- **Configuring Multiple-configuration Booting**
- **Configuring Automatic Configuration File Backup to a Remote Server**
- **Rolling Back System Configurations**
- **Saving the Configuration**

1.11.2 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: *file-name*

1.11.3 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.

2. Restrictions and Guidelines

- The startup configuration file name can be a file name or an existing path. For example, if the startup configuration file name is set to **flash:/Hostname/Hostname.text** or **usb0:/Hostname/Hostname.text**, **flash:/Hostname.** The file folder **flash:/Hostname** and **usb0:/Hostname** must exist, or the **write** command will fail to save the configurations. In the master-slave mode, the paths must exist on all devices.
- 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.
- 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 the 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:***file-name* | **usb0:***file-name* }

The saving path and name of the startup configuration file is **flash:/config.text** by default.

1.11.4 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 { **ftp** *server* [**port** *port-number*] **username** *username* **password** { [0] *password* | 7 *encrypted-password* } | **tftp** *server* } **interval** *interval-time* [**path** *folder*]] [**vrf** *vrf_name*]

The automatic configuration file backup function is not configured by default.

1.11.5 Rolling Back System Configurations

1. Overview

The configuration rollback feature allows a network administrator to create a snapshot of the current configuration, which is a copy or checkpoint of the current running configuration. The checkpoint configuration is re-applied to the device without the need for a restart.

2. Restrictions and Guidelines

- Configuration rollback is used in the following scenarios:
  - You need to copy the configuration file from another device to the new device and apply the configuration without restarting the device.
  - When current system configuration contains too many errors and it is difficult to locate faults or roll back the configuration one by one, you must roll back the current configurations to the previously correct state.
  - When the device application environment changes and the device needs to run the configuration in a configuration file, you can roll back the current configuration to the specified configuration file state without restarting the device.
- When configuration rollback is performed, the system compares and processes the current configuration with the configuration in the rollback checkpoint or configuration file:
  - For the same commands in both configurations, the system does not process them.
  - For the commands only in the current configuration, the system cancels them.
  - For commands that exist in the rollback checkpoint or configuration file but not in the current configuration, these commands will be executed.
  - For the different commands between both the current configuration and checkpoint configuration, the system cancels the configuration, and then runs related commands in the checkpoint configuration.
- This command is used to roll back the configuration from the configuration file. Commands are identified by

indentation during rollback. Incorrect indentation may cause a rollback exception. Therefore, the indentation format of the configuration file must be consistent with the format displayed in the command output of the **show running-config** command.

- Only one user can create checkpoints and configure rollback on a device at a time.
- It is recommended that you check whether the baud rate of the serial port is consistent between the current system configuration and checkpoint configuration before you perform rollback. If they are inconsistent, you are advised to change the baud rate of the serial port to that of the checkpoint configuration. Otherwise, the baud rate may change during rollback, causing a failure to display the rollback process information.
- During configuration rollback, do not hot swap any supervisor module or line card, and ensure that the device topology environment is the same as the environment for 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 the system displays the message "Increased configuration:" after rollback, the configuration increases compared with the checkpoint configuration. This is because some commands cannot be reversed or fail to be reversed. For details, see the corresponding command reference, and manually reverse these commands.
- If the system displays the message "Decreased configuration:" after rollback, the configuration decreases compared with the checkpoint configurations. This is because some commands fail to be executed during rollback. For details, see the corresponding command reference, and manually run these commands.

3. Configuration Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Roll back configurations. Perform either of the following configurations.

- Roll back the configuration through the configuration file.

  Copy the configuration file to the device.

  copy *source-url destination-url*

  The configuration is rolled back from the configuration file.

  rollback running-config config-file *file-name*

- Roll back the configuration through the checkpoint configuration.

  Create a checkpoint.

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

  No checkpoint is configured by default.

  Roll back the configuration through the checkpoint configuration.

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

1.11.6 Saving the Configuration

1. Overview

The device supports manual saving and automatic saving. The running configuration is not saved by default, and the device will use the startup configuration file after restarting. Therefore, you are advised to use this function in time to save the running configuration to the startup configuration file

2. Procedure

(1) Enter the privileged EXEC mode.

enable

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

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

1.11.7 Configuring the Login Failure Recording Function

4. Overview

The login failure recording function is enabled by default. You can run the **show login fail-record** command to display the login failure information recorded. You can also configure the maximum number of entries that can be recorded and disable the recording function.

5. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable the login failure recording function.

no login fail-record enable

The login failure recording function is enabled by default.

(4) Configure the maximum number of entries that can be recorded.

login fail-record size

The maximum number of login failure records is 512 by default.

1.12 Configuring a Restart Policy

1.12.1 Configuration Tasks

The restart policy configuration includes the following tasks:

- Configuring Immediate Restart
- Configuring Scheduled Restart

1.12.2 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

1.12.3 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. 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

1.13 Configuring a Memory Usage Threshold

1.13.1 Overview

A memory usage threshold is used to monitor the memory status of a device. Excess of this threshold may cause service exceptions. If the actual memory usage exceeds this threshold, a syslog alarm is generated. For example, if the configured memory usage threshold is 90%, when this threshold is exceeded, a syslog alarm is generated.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a memory usage threshold.

memory low-watermark set *memory-threshold*

The default memory usage threshold is **90%**.

1.14 Configuring a CPU Usage Threshold

1.14.1 Overview

When the CPU usage of the device is above the upper threshold, a CPU usage overlimit alarm is triggered. The default CPU usage upper threshold is 85%. When the CPU usage of the device drops below the lower threshold, a CPU usage restore notification is triggered. The default CPU usage lower threshold is 75%. If the default upper threshold and lower threshold for the CPU usage do not need actual needs, you can adjust the thresholds accordingly.

1.14.2 Restrictions and Guidelines

- The configuration takes effect immediately.
- The upper threshold and lower threshold for the CPU usage are synchronized to all cards in-position. All the cards use the same upper threshold and lower threshold for the CPU usage.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the upper threshold and lower threshold for the CPU usage.

cpu high-watermark set [**down** *down-value* | **up** *up-value*] ***

The default upper threshold and lower threshold for the CPU usage are 85% and 75%, respectively.

1.15 Configuring System Version Monitoring

1.15.1 Overview

After you enable system version monitoring, the device can detect the version number changes of all the cards in the cluster. If the version number of a card changes, a Syslog alarm is generated. System version monitoring helps you determine whether the versions of cards on the device are reliable.

1.15.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enable or disable system version monitoring.

monitor-version { **disable** | **enable** }

System version monitoring is disabled by default.

1.16 Monitoring and Maintenance

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

Run the **clear** command to delete all types of information.

⚠ Caution

Running the **clear** command while a device is running may cause service interruption due to the loss of important information.

Table 1-2 Monitoring and Maintenance of Basic Management

Command	Function
clear checkpoint database	Clears checkpoints and related data.
clear enable user-block { **all** | **no-user** | *user* }	Unlocks users who are locked because the number of consecutive authentication failures to enter the privileged EXEC mode exceeds the limit.
clear telnet ip-block { **all** | [*ipv4-address* | *ipv6-address*] }	Clears entries about blocked IP addresses and authentication failures.
memory history clear { **all** | **half** | **one-forth** }	Clears historical memory usage records.
memory low-watermark set *memory-threshold*	Enables the monitoring of memory usage threshold.
show boot config	Displays the saving path and name of startup configuration file.
show calendar	Displays the hardware time of the system.

Command	Function
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 configuration change running-config startup-config	Displays the differences between the running configuration file and startup configuration file.
show cpu [**core** | **slot** [*slot-id* | **all-info**]]	Displays CPU usage information of system tasks on control cores and non-virtual cores.
show cpu-monitor history [**slot** { *slot-id* | **all-info** }]	Displays the CPU usage excess history of the device.
show cpurule all	Displays the CPU rule configuration.
show debugging	Displays information about enabled debugging functions.
show enable user-block	Displays users who are blocked from privileged EXEC mode authentication on the device.
show hostname	Displays the host name of the device.
show language character-set	Displays the current character set encoding format of the device.
show line { **console** *line-number* **| vty** *line-number* **|** *line-number* }	Displays the line configurations.
show login fail-record	Displays the device login failure information recorded.
show memory [*process-id* | *process-name* | **history** | **low-watermark** | **slot** [*uslot* [**sorted total**] | *all-info* [**sorted total**]] | **sorted total**]	Displays memory information.
show memory vsd *vsd-id*	Displays Virtual Storage Director (VSD) information.
show memory-monitor history [**slot** { *slot-id* | **all-info** }]	Displays the memory usage excess history of the device.
show pci-bus	Displays information about devices mounted on the Peripheral Component Interconnect (PCI) bus.
show processes cpu [[**15min** | **1min** | **5min** | **5sec**] [**nonzero**] [**record**] | **history** [**table**]]	Displays system tasks by VSD.
show processes cpu detailed { *process-id* | *process-name* }	Displays details about a specific task.
show processes vsd *vsd-id* **cpu**	Displays details about a specific task.

Command	Function
show reload	Displays system restart settings.
show running-config [**interface** *interface-type interface-number* | **router** { **bgp** | **isis** | **ospf** }]	Displays the running configurations of the device system or configurations of an interface.
show service	Displays the service status (enabled/disabled).
show sessions	Displays information about established Telnet client instances.
show startup-config	Displays the device configurations stored in the NVRAM.
show sysmon grpc info	Displays information about the gRPC function registered in the system monitoring process.
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 usb-bus	Displays information about devices mounted on the USB bus.
show version [**detail**]	Displays system information.
show monitor-version status	Displays whether system version monitoring is enabled.

1.17 Configuration Examples

1.17.1 Configuring Login Authentication and Telnet Service

1. Requirements

You can use Device A as a jump server through the workstation to manage Device B remotely.

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

2. Topology

Figure 1-1 Configuring the Telnet Service

3. Notes

- Establish a Telnet session to the remote device whose IPv4 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 on Device B.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# line vty 0
Hostname(config-line)# password Abc123456
Hostname(config-line)# login
```

(2) Establish a telnet session to a remote device on Device A.

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

```
Hostname# telnet 192.168.65.119
Trying 192.168.65.119 ... Open
User Access Verification
Password: Abc123456
Hostname# telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password: Abc123456
Hostname(config)# do telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password: Abc123456
```

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.

1.17.2 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
```

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 2
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 3
1.4.1 Overview 3
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 9
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.

(4) Return to the global configuration mode.

exit

(5) Enter the line configuration mode.

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

(6) 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**.

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 interface configuration mode of the role.

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 interface configuration mode of the role.

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 VLAN configuration mode of the role.

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 VLAN configuration mode of the role.

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 VRF configuration mode of the role.

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
debug rbac	Debugs the RBAC module.
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 [**name** *group-name*] [**detail**]	Displays the basic information or details about a specific feature group or all feature groups.

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 **Abc123456**, 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 **Abc123456**. 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 **Abc123456**, 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 **Abc123456**, and assign the user with the role **test**.

```
DeviceA(config)# username user password Abc123456
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 $10$184$HItkSIIBDRBo$
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 9
1.7.1 Configuring Line Attributes 9

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

line maximum-vty *max-number*

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

(4) Enter the line configuration mode.

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

(5) 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.

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

line maximum-vty *max-number*

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

(4) Enter the line configuration mode.

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

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

Note

The **access-class** and **ipv6 access-class** commands cannot be run on **line console 0**.

(IPv4 network)

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

(IPv6 network)

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

No ACL is configured for controlling terminal login by default.

(6) (Optional) Enable accounting for a line. All the following configurations are optional and may be selected as needed.

- Enable command accounting for a line.

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

  The command accounting function is disabled by default.

- Enable user access accounting for a line.

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

The user access accounting function is disabled by default.

- Enable command authorization for a line.

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

  The command authorization function is disabled by default.

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

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

The EXEC authorization function is disabled by default.

(8) Configure the access to the CLI through a line.

exce

Accessing the CLI through lines is enabled by default.

(9) 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 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 for a line is disabled by default.

- 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 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 access to the CLI through a line.

  exce

  Accessing the CLI through lines is enabled by default.

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

length *screen-length*

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

- Configure location description for a specific line.

  location *location*

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

- Enable logging display on terminals.

  monitor

  Logging display on terminals is disabled by default.

- Configure a privilege level for line-based login.

  privilege level *privilege-level*

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

- 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 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 terminal connected to a specified line, that is, the line width.

  width *screen-width*

  The line width is **79** by default.

(10) 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**.

1.5 Configuring Terminal Attributes

1.5.1 Overview

This section describes how to configure terminal attributes.

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.

- 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 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.

- Configure the baud rate for the current terminal.

  terminal speed *baudrate*

  The default baud rate is **9600**.

- 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 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 history all-users	Clears historical records.
clear line { *line-number* | **console** *console-line-number* | **vty** *vty-line-number* }	Clears the connection status of a line.
show enable password	Displays the authorization password in JSON format.
show history	Displays historical command records of a line.

Command	Purpose
show history all-users	Displays all historical command records.
show line { *line-number* | **console** *console-line-number* | **vty** *vty-line-number* }	Displays the line configurations.
show privilege	Display the privilege level of a line.
show user [**all**]	Displays login user information of a line.
show web-api line vty info	Displays the VTY configuration information in JSON format.

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

(1) 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 vty 0 6
Device(config-line)# access-class acl1 in
```

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

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

(3) Set the baud rate to 115200 bps.

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

(4) Set the number of data bits to **8**.

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

(5) Set the parity bit to **even**.

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

(6) Set the number of stop bits to **1**.

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

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

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

(8) Configure software flow control.

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

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

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

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

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

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

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

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

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

(13) Configure the user verification method.

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

(14) Configure a username.

```
Device(config)# username Device privilege 15 password Abc123456
```

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 $10$184$HItkSIIBDRBo$
!
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 $10$184$HItkSIIBDRBo$
 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
1.4.9 Formatting a Flash Memory Disk....6

1.5 Monitoring 6

1.6 Configuration Examples 7

1.6.1 Configuring Basic Features of File System Management 7

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
  - Formatting a Flash Memory Disk

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* | **startup-config** }

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**]

The prompt level for operating a file is **noisy** by default.

1.4.9 Formatting a Flash Memory Disk

1. Overview

This feature formats a Flash memory disk.

2. Restrictions and Guidelines

The device restarts after this feature is executed. After that, the Flash partition is formatted. Then, all files except the configuration files in the flash partition are deleted. Before formatting the flash disk, you are advised to back up important files in the flash partition.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Format a Flash memory disk.

format flash

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 coredump files	Displays the Coredump file information of a card in-position.
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

1 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 USB 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 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

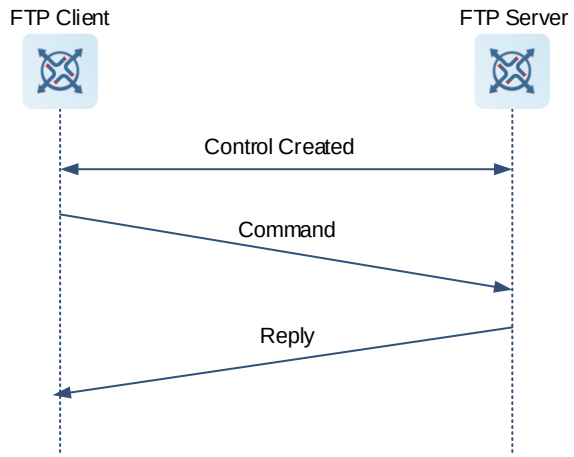
1. FTP Connection

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

- RFC 959: File Transfer Protocol (FTP)
- RFC 3659: Extensions to FTP
- RFC 2228: FTP Security Extensions
- RFC 2428: FTP Extensions for IPv6 and NATs
- RFC 1635: 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 after you enter an incorrect username or password for three times 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.

- Configure the maximum number of login verification times allowed by the FTP lock function.

  ftp-server login block failed-times *times*

  By default, the maximum number of login verification times allowed by the FTP lock function is 3.

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*.

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

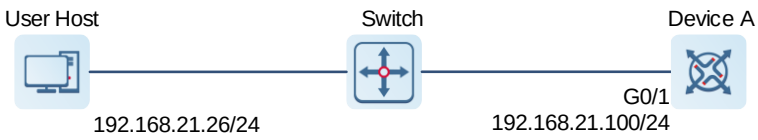
1.9.1 Providing the FTP Service in a LAN

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 **Abc123456**.

(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 0/1
DeviceA(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 **Abc123456**.

```
DeviceA(config)# ftp-server username user password Abc123456
```

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)$10$184$HItkSIIBDRBo$
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 $10$184$HItkSIIBDRBo$
!
```

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 4
1.3.1 Overview 4
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*.

The following sections introduce only the FTP client.

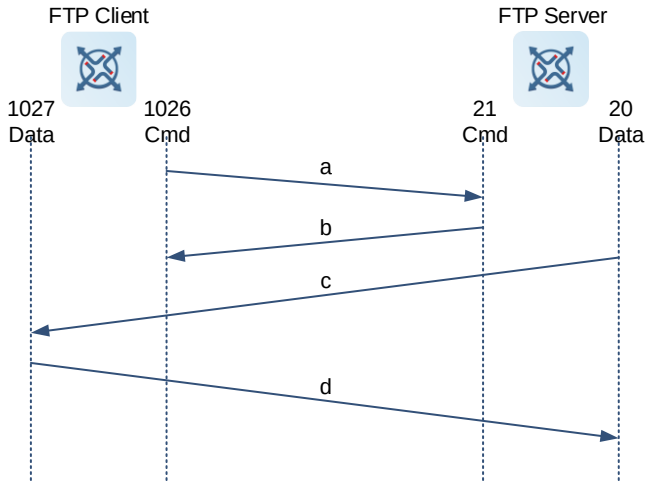
1.1.2 Principles

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. 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:

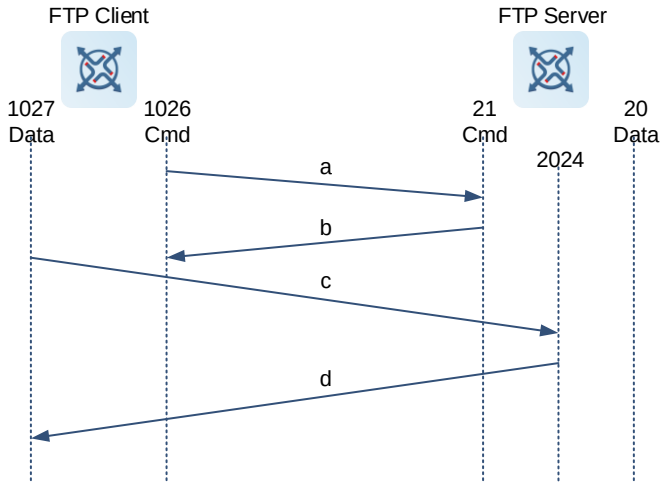
  a The FTP client establishes a control channel through port 1026 and port 21 of the FTP server, and sends control commands through this channel.

  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

- RFC 959: 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) Upload files.

copy flash:*local-file* { **ftp:** }***//****account-information@remote-file*

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) (Optional) Disable the size check of files downloaded from the FTP server.

- Enter the global configuration mode.

  configure terminal

- 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.

- Exit the global configuration mode.

  exit

(3) Download files.

copy { **ftp:** }***//****account-information@remote-file* **flash:***local-file*

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*.

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*.

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*] **ascii**

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*.

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

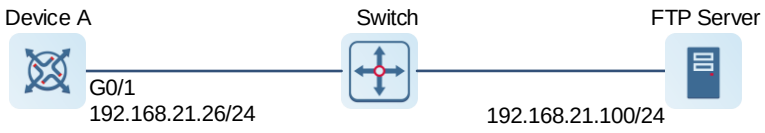
1.9.1 Configuring the FTP Client

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 Topology of FTP Client



3. Notes

- Set the FTP connection mode to PORT.
- Set the transmission mode to ASCII.
- Use the username **user** and password **Abc123456** 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 **Abc123456** 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.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# ip address 192.168.21.26 255.255.255.0
Device A(config-if-GigabitEthernet 0/1)# exit
```

b. Set the transmission mode to ASCII.

```
Device A(config)# ftp-client ascii
```

c. Set the FTP connection mode to PORT.

```
Device A(config)# ftp-client port
Device A(config)# exit
```

d. Upload the file.

```
Device A# copy flash: home/local-file
ftp://user:pass@192.168.21.100/root/remote-file
```

e. Download the file.

```
Device A# 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.

```
Device A> enabl
Device A# show ftp-client
      ftp-client information
==================================
type: ASCII
mode: PORT
```

6. Configuration Files

Device A configuration file

```
hostname Device A
!
interface gigabitEethernet 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 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 Monitoring 3

1.3 Configuration Examples 4

1.3.1 Configuring the TFTP Server 4

1 Configuring 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

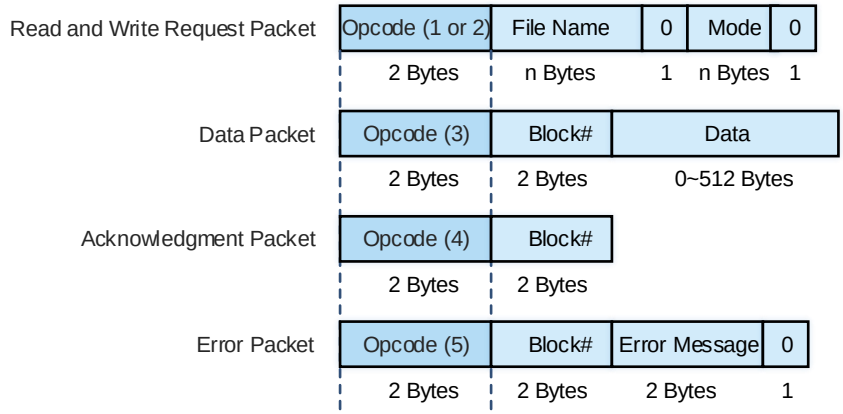
After the TFTP client initiates a file read or write request, and the TFTP server approves the request, TFTP transmits the data in 512-byte packets. A packet with less than 512 bytes indicates that the transmission is completed.

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

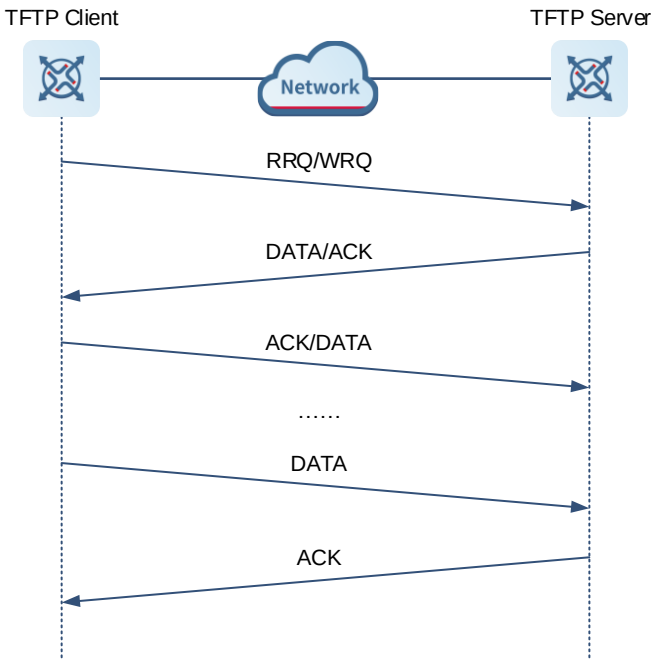


The Error Message in an error packet contains 2 bytes in ASCII code. TFTP provides the following error codes:

- 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

- RFC 1350: The TFTP Protocol (revision 2)
- RFC 2347: TFTP Option Extension
- RFC 2348: TFTP Blocksize Option
- RFC 2349: TFTP Timeout Interval and Transfer Size Options

1.2 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.

1.3 Configuration Examples

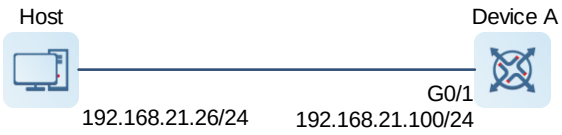
1.3.1 Configuring the TFTP Server

1. Requirements

Configure a TFTP server in a LAN so that users can upload and download files.

2. Topology

Figure 1-3 Topology of 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 Ethernet interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.21.100 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# 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 gigabitEthernet 0/1
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 2
1.3.1 Overview 2
1.3.2 Restrictions and Guidelines 2
1.3.3 Procedure 2
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 Configuring a Port Number for TFTP Connection 3
1.6.1 Overview 3
1.6.2 Restrictions and Guidelines 3
1.6.3 Procedure 3
1.7 Monitoring 3

1.8 Configuration Examples.....4

1.8.1 Configuring the TFTP Client 4

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

1. Specifying the Source Interface IP Address for TFTP Transmission

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.

2. Specifying a Port Number for Connection with the TFTP Server

You can specify a port number on the TFTP client to connect with the TFTP server and transfer files. Specifying a port number also prevents attacks.

1.1.3 Protocols and Standards

- RFC 783: Trivial FILE TRANSFER PROTOCOL (TFTP)

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Basic functions of the TFTP client
  - Enabling the TFTP Client to Upload Files
  - Enabling the TFTP Client to Download Files
- Extended functions of the TFTP client
  - Binding the Source IP Address to the TFTP Client
  - Configuring a Port Number for TFTP Connection

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) Upload files.

copy flash:*local-file* { **tftp:** }***//****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) Download files.

copy { **tftp:** }***//****remote-file* **flash:***local-file*

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 Configuring a Port Number for TFTP Connection

1.6.1 Overview

You can specify the port number used by the TFTP client to connect with the TFTP server for file upload and download.

1.6.2 Restrictions and Guidelines

The range of the port number configured for the TFTP client is from 20000 to 65534.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the port number used by the TFTP client to connect with the TFTP server.

tftp-client port *port-number*

The default port number used by the TFTP client to connect with the TFTP server is **69**.

1.7 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.

1.8 Configuration Examples

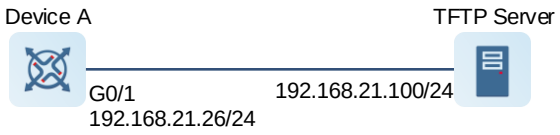
1.8.1 Configuring the TFTP Client

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 Topology of 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 **download-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: download-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 **download-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 HTTP....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 of HTTP Service....3
1.3.1 Overview....3
1.3.2 Restrictions and Guidelines....3
1.3.3 Procedure....4
1.4 Configuring Remote HTTP Upgrade....4
1.4.1 Overview....4
1.4.2 Restrictions and Guidelines....4
1.4.3 Procedure....5
1.5 Monitoring....5
1.6 Configuration Examples....6
1.6.1 Configuring Basic Features of HTTP Service....6
1.6.2 Configuring Remote HTTP Upgrade....7

1 Configuring HTTP

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:

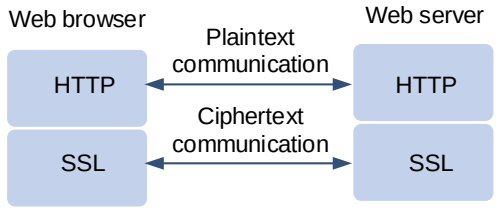
- A TCP connection is established between the client and the server. The default port number of the HTTP service is 80 and the default port number of the HTTPS service is 443.
- The client sends a request to the server.
- The server parses the request sent by the client. The request content includes 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 Certificate

The HTTPS certificate is used for server identity verification and encrypted data transmission. You can regenerate a self-signed certificate on the device or install the trusted certificate applied from the Certificate Authority (CA). If the HTTPS certificate is not trusted by the browser, a security prompt is displayed when you access the Web management page of the device using HTTPS over the browser. You need to confirm the prompt before you can continue your access. The working principles are as follows:

(1) The device automatically generates a self-signed certificate as the HTTPS certificate upon first power-on. You can regenerate a self-signed certificate on the device or install the trusted certificate applied from the CA.

(2) After the browser connects to the server through HTTPS, the server sends the certificate to the browser.

(3) The browser verifies the certificate information sent by the server to check whether the certificate user matches the access address, whether the certificate is valid, and whether the certificate issuer is trusted by the browser. If not, the browser displays a security prompt. You need to confirm the prompt or add the certificate as a trusted one before you can further access the server.

4. Automatic Switching from HTTP to HTTPS

After automatic switching from HTTP to HTTPS is enabled, the device redirects the access request of the browser to HTTPS when you access the Web management page of the device using HTTP over the browser. The working principles are as follows:

(1) After you enter an HTTP address such as http://192.168.1.1 in the browser, the browser initiates an HTTP access request to the device.

(2) The device replies to the HTTP access request and redirects to an HTTPS address such as https://192.168.1.1.

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

5. HTTP Upgrade Service

Two HTTP upgrade methods are available: local HTTP upgrade and remote HTTP upgrade.

- Local Upgrade Service

  When the device functions as an HTTP server, you can log in to the device from the Web browser to upload files to be upgraded (including component packages and Web packages) to the device or directly upload the files to the device using Trivial File Transfer Protocol (TFTP). The working principles are as follows:

  a Upload component packages or Web packages using the local upgrade function on the Web system.

  b The device receives the files and verifies the file versions and validity.

c After successful file verification, directly upgrade the Web packages or determine whether to upgrade the component packages by selecting whether to restart the device.

- Remote Upgrade Service

  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. If the server address is not connected, connect the device to the server address in the local upgrade file.

  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

- RFC 1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2818: Hypertext Transfer Protocol Over TLS -- HTTPS

1.2 Configuration Task Summary

HTTP service configuration includes the following tasks:

(1) Configuring Basic Features of HTTP Service

(2) Configuring Remote HTTP Upgrade

1.3 Configuring Basic Features of HTTP Service

1.3.1 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.

1.3.2 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.
- Currently, the service supports multi-user management and simultaneous login for multiple accounts; you can use one account to log in to multiple ends simultaneously (multiple browsers and so on).
- Users can configure an HTTPS service port number to reduce attacks initiated by unauthorized users on

HTTPS service.

- During the login, if you do not operate the Web page for more than 30 minutes, you will log out due to time out and need to log in again.

1.3.3 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.

(7) (Optional) Delete the default username.

no webmaster default-username

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 may not be configured because the local upgrade record file records the addresses of possible upgrade servers.
- 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 daily** 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.

1.4.3 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* | *ipv4-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) Exit to the privileged EXEC mode.

end

(7) (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.

(8) 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.

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 7 Abc123456
```

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
```

6. Configuration Files

```
hostname Device
!
http port 8080
http secure-port 4430
enable service web-server http
enable service web-server https
web-server http redirect-to-https
web-server https generate self-signed-certificate
webmaster level 1 username test1 password 7 $10$184$HItkSIIBDRBo$
!
interface GigabitEthernet 0/1
 no switchport
 ip address 1.1.1.10 255.255.255.0
!
end
```

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.

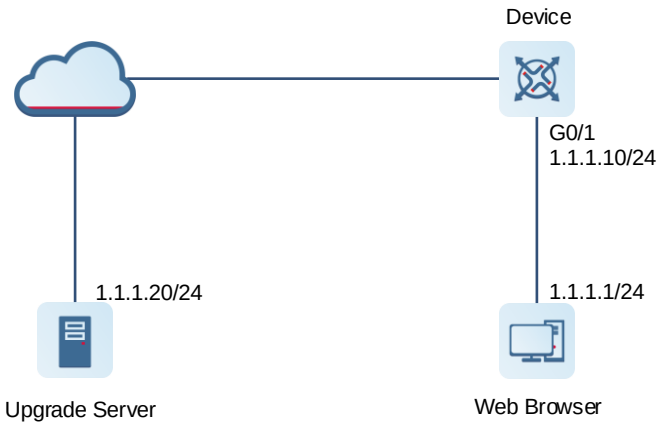
1.6.2 Configuring Remote HTTP Upgrade

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.
- Set the scheduled time for the device to remotely check for upgrade files on the upgrade server to 02:00 every day.
- The device checks for upgrade files on the upgrade server.
- The device downloads the latest file from the HTTP upgrade server and updates.

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 1.1.1.20
Sending 5, 100-byte ICMP Echoes to 1.1.1.20, 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 domain-lookup
ip name-server 192.168.58.110
!
enable service web-server http
enable service web-server https
http update time daily 02:00
!
interface GigabitEthernet 0/1
 no switchport
 ip address 1.1.1.10 255.255.255.0
!
end
```

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 RFC3164 Log Format 2
1.1.6 RFC5424 Log Format 6
1.1.7 System Log Filtering 8
1.1.8 Log Reporting 9
1.1.9 Configuring System Log Monitoring 10
1.1.10 Protocols and Standards 10
1.2 Configuration Task Summary 10
1.3 Configuring Basic Syslog Features 11
1.3.1 Overview 11
1.3.2 Procedure 11
1.4 Configuring the System Log Format 11
1.4.1 Overview 11
1.4.2 Configuration Tasks 11
1.4.3 Configuring the RFC3164 Log Format 11
1.4.4 Configuring the RFC5424 Log Format 12
1.4.5 Configuring a Space Next to <pri> in the Log Format 13

1.4.6 Configuring the Log Format to Carry Identity Information 13
1.5 Configuring Log Reporting 14
1.5.1 Configuration Tasks 14
1.5.2 Restrictions and Guidelines 14
1.5.3 Configuring Level-based Log Reporting 14
1.5.4 Configuring Delayed Log Reporting 14
1.5.5 Configuring Periodical Log Reporting 16
1.6 Configuring System Log Monitoring 17
1.6.1 Overview 17
1.6.2 Restrictions and Guidelines 17
1.6.3 Procedure 17
1.7 Configuring the Output Direction of System Logs 18
1.7.1 Configuration Tasks 18
1.7.2 Configuring the Output of System Logs to the Console 18
1.7.3 Configuring the Output of System Logs to the Monitor Terminal 19
1.7.4 Configuring the Function of Writing System Logs into the Memory Buffer 19
1.7.5 Configuring the Transmission of System Logs to the Log Server 20
1.7.6 Configuring the Function of Writing System Logs into Log Files 21
1.8 Configuring System Log Filtering 23
1.8.1 Overview 23
1.8.2 Restrictions and Guidelines 23
1.8.3 Procedure 23
1.9 Configuring System Log Redirection 24
1.9.1 Overview 24

1.9.2 Restrictions and Guidelines 24
1.9.3 Procedure 25
1.10 Configuring Performance Logging Function 25
1.10.1 Overview 25
1.10.2 Restrictions and Guidelines 25
1.10.3 Procedure 25
1.11 Configuring Synchronization of User Input and Log Output 25
1.11.1 Overview 25
1.11.2 Restrictions and Guidelines 26
1.11.3 Procedure 26
1.12 Monitoring 26
1.13 Configuration Examples 27
1.13.1 Configuring the RFC3164 Log Format 27
1.13.2 Configuring the RFC5424 Log Format 30

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.

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 RFC3164 Log Format

Formats of system logs may vary with the system log output direction.

1. Non-server Direction

When logs are output to the console, monitor terminal, log buffer, or log file, the system logs are in the following format:

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

The log format is described below:

Sequence number: *timestamp: system name %module name-severity-mnemonic: log text

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

```
001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

2. Server Direction

When logs are output to the log server, the system logs are in the following format:

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

The log format is described below:

<Priority> sequence number: *timestamp: system name %module name-severity-mnemonic: log text

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

```
<189>001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

The following details each field in the log format:

- priority

  The priority is calculated using the following formula: Facility x 8 + Level. "Level" indicates the log level and "Facility" indicates the numerical code of the facility. The default facility value is local7 (23). Table 1-3 lists the value range of the facility.

Note

This field is valid only when logs are output to the log server.

Table 1-3 Description of the Log Priority Parameter

Numerical Code	Facility Keyword	Facility Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth1	Security/Authorization messages
5	syslog	Messages generated internally by syslog
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	clock1	Clock daemon
10	auth2	Security/Authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem

Numerical Code	Facility Keyword	Facility Description
13	logaudit	Log audit
14	logalert	Log alert
15	clock2	Clock daemon
16	local0	Local use 0 (local0)
17	local1	Local use 1 (local1)
18	local2	Local use 2 (local2)
19	local3	Local use 3 (local3)
20	local4	Local use 4 (local4)
21	local5	Local use 5 (local5)
22	local6	Local use 6 (local6)
23	local7	Local use 7 (local7)

- seq no (sequence number)

  The sequence number of a system log is a 6-digit integer, and increases with system logs. By default, the sequence number is not displayed. You can run a command to display or hide this field.

- timestamp

  The timestamp records the generation time of a system log to help you check and locate system events. The devices support two formats of system log timestamps: datetime and uptime.

  - Datetime format

  The complete datetime format is as follows:

  ```
  Mmm dd yyyy hh:mm:ss.msec
  ```

  Table 1-4 describes each parameter of the timestamp in the datetime format.

  - uptime format:

  The complete uptime format is as follows:

  ```
  dd:hh:mm:ss
  ```

  Table 1-5 describes each parameter of the timestamp in the uptime format.

Table 1-4 Description of Parameters in the Timestamp in the Datetime Format

Timestamp Parameter	Parameter Name	Description
Mmm	Month	Indicates the abbreviated month. The 12 months in a year are abbreviated as Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
dd	Day	Indicates the day in the current month.

Timestamp Parameter	Parameter Name	Description
yyyy	Year	Indicates the year, not displayed by default.
hh	Hour	Indicates the hour.
mm	Minute	Indicates the minute.
ss	Second	Indicates the second.
msec	Millisecond	Indicates the millisecond.

Note

By default, the timestamp in the datetime format in system logs does not contain the year and milliseconds. You can run a command to display or hide the year and millisecond in the timestamp in the datetime format.

Table 1-5 Description of Parameters in the Timestamp in the Uptime Format

Timestamp Parameter	Parameter Name	Description
dd	Day	Indicates the day in the month in which the device starts up.
hh	Hour	Indicates the hour at which the device starts up.
mm	Minute	Indicates the minute at which the device starts up.
ss	Second	Indicates the second at which the device starts up.

Note

If the device does not have a real time clock (RTC), which is hardware used to record the absolute time of the system, the device uses its startup time (in the uptime format) as the system log timestamp by default. If the device has an RTC, the device uses its absolute time (in the datetime format) as the system log timestamp by default.

- sysname (system name)

  This field records the name of the device that generates a log so that the log server can identify the host of such device. By default, the field is not displayed. You can run a command to display or hide this field.

- 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 a string of 4 to 64 characters, which can contain upper-case and lower-case letters, digits, and underscores. The **mnemonic** field is mandatory for common logs by default, and optional for debugging logs.

- content (log text)

  This field indicates the content of a system log.

1.1.6 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 x 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. The devices use the following uniform timestamp format when the RFC5424 logging function is enabled:

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

  Table 1-6 describes each parameter.

Table 1-6 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".

Timestamp Parameter	Parameter Name	Description
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 a string of 4 to 64 characters, which can contain upper-case and lower-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 1-7 describes each parameter.

Table 1-7 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.

Structured Parameter	Parameter Name	Description
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). The enterprise ID of 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.

1.1.7 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.

1.1.8 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.

1.1.9 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.

1.1.10 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. The configurations below are mutually exclusive. Configure either of the tasks.

- Configuring the RFC3164 Log Format
- Configuring the RFC5424 Log Format
- Configuring a Space Next to <pri> in the 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 Configuration Tasks

System log format configuration includes the following tasks. The following configurations are mutually exclusive. Configure either of the tasks.

- Configuring the RFC3164 Log Format
- Configuring the RFC5424 Log Format
- Configuring a Space Next to <pri> in the Log Format

1.4.3 Configuring the RFC3164 Log Format

1. Restrictions and Guidelines

- If the device does not have an RTC, which is hardware used to record the absolute time of the system, the system uses the device startup time (in the **uptime** format) as the log timestamp. In this case, the configured device time is invalid. If the device has an RTC, the system uses the device time (in the **datetime** format) as the log timestamp.
- Add a system name to logs to identify the device that generates a system log after the system log is sent to the server.
- Add a sequence number to logs. The sequence number starts from 1. After the sequence number is added, the system can monitor the loss and the generation sequence of logs. The log sequence number is a 6-digit integer. Each time a log is generated, the sequence number increases by one. When the sequence number increases from 1 to 1,000,000, or reaches 2^32, it starts from 000000 again.
- After the RFC3164 format is enabled, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable to the RFC5424 format will become invalid and be hidden.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the timestamp format for system logs.

service timestamps [*message-type* [**datetime** [**msec** | **year**] * | **uptime**]]

The system logs use the datetime timestamp format, and the timestamp does not contain the year and milliseconds by default.

(4) (Optional) Add the system name to system logs.

service sysname

By default, system logs do not contain the system name.

(5) (Optional) Add the sequence number to system logs.

service sequence-numbers

By default, system logs do not contain the sequence number.

(6) Configure the system log format. The configurations below are mutually exclusive. Configure one of the log formats.

- Set the system log format to the standard log format.

  service standard-syslog

- Set the system log format to the private log format.

  service private-syslog

1.4.4 Configuring the RFC5424 Log Format

1. 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.
- After the RFC5424 format is enabled, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable to the RFC3164 format will become invalid and be hidden.

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

1.4.5 Configuring a Space Next to <pri> in the Log Format

1. Restrictions and Guidelines

- If there is no special requirement, configure a space on the device that needs a space next to <pri> in the log format.
- The default format of logs sent to a server are as follows:

```
<pri>*timestamp: %module-level-mnemonic: content
```

The order is as follows:

```
<pri>*timestamp: %module-level-mnemonic: content
```

If the function is enabled, the format of logs sent to a server are as follows:

```
<pri> *timestamp: %module-level-mnemonic: content
```

Compared with the default log format, a space is added next to <pri>.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a space next to <pri> in the log format.

logging priv-format private

By default, no space exists after <pri> in the log format.

1.4.6 Configuring the Log Format to Carry Identity Information

1. Restrictions and Guidelines

- Unless otherwise specified, configure this function to carry identity information in the log format in the RFC3164 format.
- The default format for logs sent from the device to the server is as follows:

```
<pri>*timestamp: %module-level-mnemonic: content
```

The following describes the preceding parameters:

```
<Priority>*Timestamp: %Module name-Level-Mnemonic: Log content
```

If this function is configured, the log sent from the device to the server is displayed in the following format:

```
<pri>Origin-id: *timestamp: %module-level-mnemonic: content
```

The following describes the preceding parameters:

```
<Priority>Identity information: *Timestamp: %Module name-Level-Mnemonic: Log content
```

The identity information is added.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the log format to carry identity information.

logging origin-id { **hostname** | **string** *word* }

By default, logs do not carry identity information.

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 { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-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 [**console**] [**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 10 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.
- 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.
- The **logging trap** command is used to configure the severity level of logs that are sent to all syslog servers on a device. The log severity level configured in the **logging server** command is used for each device to determine whether to send logs to all syslog servers. Logs generated by the device can be sent to the corresponding log server only when the level is smaller than or equal to the log severity level specified in both the **logging trap** command and the **logging server** command. For details about the severity levels of logs, see Table 1-1. A smaller value indicates a higher severity level.
- The priority carried in the logs sent by the device to the log server is specified by the **facility-type** parameter in the **logging facility** command. The **facility-type** parameter in this command is only used to determine whether to send logs to the log server. If the value specified in this command is greater than or equal to the value specified in the **logging facility** command, the device can send system logs to the log server. Otherwise, the device cannot send system logs to the log server.

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.

logging server { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-port** *port-number*] [**facility** *facility-type*] [**level** *inform-level*]**logging** { *ipv4-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] [**udp-port** *port-number*] [**facility** *facility-type*] [**level** *inform-level*]

No syslog server is specified to record logs by default.

(4) (Optional) Configure the severity level of logs that are sent to the syslog server.

logging trap [*severity-level*]

The default severity level of logs is 6 (informational messages). Logs of levels 0 to 6 can be sent to the log server.

(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.
- You can configure an upper alarm threshold for the system log storage space based on actual needs to back up historical logs in time and prevent log loss because some logs are overwritten. When the storage space accumulatively occupied by log files reaches the configured upper alarm threshold, the system generates Syslog and trap alarms and instructs you to back up the logs in time. After you back up and delete the logs, the system checks the occupied space again. If the occupied space is below the threshold, the system generates the Syslog and trap alarms for the restoration.
- 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, 32 log files are created by default after the function of writing logs into log files is enabled. If the device has generated 32 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 32 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 32.

(5) Configure an upper alarm threshold for the system log storage space.

logging file alarm-threshold *percent-number*

The upper alarm threshold for the system log storage space is 90% by default.

(6) 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.

(7) 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.

(8) 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.
- In a VSU environment composed of chassis-type devices, after the log redirection function is enabled, logs generated by the slave or standby Supervisor Engine will be redirected to the master Supervisor Module for output, and a role flag string "(*device ID/Supervisor Engine name)" will be added to each log to indicate that

a log is a redirected log. If four Supervisor Engines are used in a VSU, the role flag strings are as follows: (*1/M1), (*1/M2), (*2/M1), and (*2/M2).

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) Enter the configuration mode of a specified line.

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

(4) 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 1-8 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.
show logging reverse [**timestamp** *YY MM DD hh:mm:ss*]	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 RFC3164 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 RFC3164 Log Format Configuration

3. Notes

- Configure the L3 network reachable between the device and the server.
- Enable logging.
- Configure the log format.
  - Set the system log format to RFC3164 format.
  - Configure the log display format.
  - Set the timestamp format to datetime and add the millisecond and year to the timestamp.
  - Add the system name to the system log format.
  - Add the sequence number to the system log format.
- Configure log monitoring.
  - Configure 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 192.168.1.20.
  - 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 gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 10.1.1.2 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
```

(2) Enable logging.

```
Device(config)# logging on
```

(3) Configure the system log format.

Set the system log format to RFC5424 log format.

```
Device(config)# no service log-format rfc5424
```

Set the log display format to standard log format.

```
Device(config)# service standard-syslog
```

Set the timestamp format to datetime and add the millisecond and year to the timestamp.

```
Device(config)# service timestamps log datetime year msec
Device(config)# service timestamps debug datetime year msec
```

Add the system name to the system log format.

```
Device(config)# service sysname
```

Add the sequence number to the system log format.

```
Device(config)# service sequence-numbers
```

(4) 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
```

(5) Synchronize user input and log output.

```
Device(config-line)#logging synchronous
Device(config-line)#exit
```

(6) Enable performance logging.

```
Device(config)# logging performance switch
```

(7) Configure 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
```

(8) 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 192.168.1.20.

```
Device(config)# logging server 192.168.1.20
```

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

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

```
Device# ping 192.168.1.20
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
```

Run the **show logging config** command to check the configuration.

```
Device# show logging config
Syslog logging: enabled
  Console logging: level informational, 82 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 83 messages logged
  File logging: level debugging, 83 messages logged
  File name:syslog.txt, size 128 Kbytes, the 1 file is currently being written
  Standard format:true
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level debugging, 82 message lines logged,8 fail
    logging to  192.168.1.20
```

6. Configuration Files

Device configuration file

```
hostname Device
!
service standard-syslog
service sysname
service sequence-numbers
service timestamps debug datetime msec year
service timestamps log datetime msec year
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 server 192.168.1.20
logging performance switch
!
interface VLAN 1
 ip address 192.168.1.10 255.255.255.0
!
end
```

1.13.2 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 1-2 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 192.168.1.20.
  - 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 gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.1.10 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# 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
Device(config)# logging delay-send server 192.168.1.20 mode ftp user admin password
Abc123456
```

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 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 192.168.1.20.

```
Device(config)# logging server 192.168.1.20
```

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 192.168.1.20
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 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, 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  192.168.1.20
  Delay-send logging: 0 message lines logged
    logging to  192.168.1.20  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 192.168.1.20
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 STAT interval 30
logging delay-send terminal
logging delay-send interval 7200
logging delay-send file flash:syslog
logging delay-send server 192.168.1.20 mode ftp user admin password
$10$184$HItkSIIBDRBo$
!
interface GigabitEthernet 0/1
 ip address 192.168.1.10 255.255.255.0
!
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 Restrictions and Guidelines 4
1.5 Configuration Task Summary 4
1.6 Configuring System Version Upgrade 4
1.6.1 Configuration Tasks 4
1.6.2 Configuring Subsystem Upgrade/Degrade 5
1.6.3 Configuring Version Auto-sync 5
1.6.4 Configuring One-click Upgrade 6
1.7 Configuring Patch Version Upgrade 7
1.7.1 Overview 7
1.7.2 Configuration Restrictions and Guidance 7
1.7.3 Configuration Tasks 7
1.7.4 Installing a Patch Package 7
1.7.5 Activating a Patch Package by One Click 8
1.7.6 Uninstalling a Patch Package 9
1.7.7 Patch Auto-Sync 10

1.8 Monitoring 10

1.9 Configuration Examples 11

1.9.1 Configuring Subsystem Upgrade 11

1.9.2 Configuring Auto-sync Upgrade 14

1.9.3 Installing a Patch Package 15

1.9.4 Uninstalling a Patch Package 18

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. 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.

- Rack package

  A rack package is used to upgrade/degrade subsystems of rack-type devices. It contains the Main packages of the supervisor modules, switch fabric modules, and line cards. The rack package allows all the modules on a rack-type device to be upgraded once for all.

- 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 modules, 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 module 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 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 Restrictions and Guidelines

If the password encryption type is 7 or 8, when the device version is downgraded to a version that does not support the AES128/SHA256 encryption algorithm, the password may not be identified. Therefore, before the device is downgraded, you must reconfigure the password as a plaintext password or a type 7 password ciphertext generated on a lower version device.

- During device upgrade, the following error message may be reported: cannot open "/dev/ubi7_0". If the device is upgraded finally, the reported error is automatically rectified. If the device fails to be upgraded, try to upgrade the device again. If the error persists, check for hardware damage.

1.5 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
  c Configuring One-click Upgrade
- Configuring Patch Version Upgrade
  - Installing a Patch Package
  - (Optional) Activating a Patch Package by One Click
  - Uninstalling a Patch Package
  - Patch Auto-Sync

1.6 Configuring System Version Upgrade

1.6.1 Configuration Tasks

System version upgrade configuration includes the following tasks:

(1) Configuring Subsystem Upgrade/Degrade

(2) (Optional) Configuring Version Auto-sync

(3) Configuring One-click Upgrade

1.6.2 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.

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 of the device because the rack package is large, and then run the **upgrade** command.
- After running the **upgrade** command to complete the upgrade of the installation package, you need to run the **reload** command to restart the device to complete the update process. Otherwise, the installation package before the upgrade will be still running on the system.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Upgrade the installation package corresponding to the device.

upgrade { *url* [**slot** *slot-id* | **slot all**] | **download** { **ftp**://path [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] | **https**://path [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] | **sftp**://path [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] | **tftp:**//*path* [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] } } [**force**]

(3) Upgrade all Uboot and Rboot files on the device.

upgrade boot { *url* [**slot** *slot-id* | **slot all**] | **download** { **ftp:**//*path* [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] | **https:**//*path* [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] | **sftp:**//*path* [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] | **tftp:**//*path* [**slot** *slot-id* | **slot all**] [**vrf** *vrf-name*] } } [**force**]

(4) Restart the device to complete the upgrade process.

reload

1.6.3 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 { **compatible** | **coordinate** | **none** }

(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*

(5) Configure the status of the version auto-sync service.

upgrade sync-server [**close** | **open**]

Automatic version synchronization is enabled by default.

1.6.4 Configuring One-click Upgrade

1. Overview

The one-click upgrade function is a method used to easily and quickly upgrade the system software of a device. In the VSU system, the traditional upgrade method requires a device restart after upgrade. ISSU upgrades the device by controlling the active/standby switchover of the device. The specific process is as follows: First, upgrade the version of the standby device and restart it. After the standby device starts with the new version, the active device becomes the new standby device. Then, upgrade the new standby device and restart it. After this, the VSU is upgraded to the target version. ISSU helps you reduce service interruption time and improve service forwarding reliability.

2. Restrictions and Guidelines

- Ensure that the device is in powered-on state during upgrade.
- This command is supported in the VSU system on rack-type devices and box-type devices. If the number of VSU members in a box-type device exceeds 2, this command is not supported.

3. Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enable the ISSU function and install a package to upgrade the device.
upgrade auto { *url* [**delay-time** *time-number*] | **download** { **ftp:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] | **https:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] | **sftp:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] | **tftp:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] } } [**force**]

(3) After all VSU members of the device restart, the device is upgraded.

1.7 Configuring Patch Version Upgrade

1.7.1 Overview

Besides the main program version, 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. RGOS provides a patching mechanism in addition to the main program version to quickly fix bugs in the main program version. The patch package can only fix the bugs in specific software versions. After the main program version is upgraded, the corresponding patch will expire automatically.

1.7.2 Configuration Restrictions and Guidance

- After the hot patch package is installed, the patch will take effect directly without restarting the device. If a cold patch package is installed, the device must be restarted for the patch to take effect.

1.7.3 Configuration Tasks

Patch version configuration includes the following tasks:

(1) Installing a Patch Package

(2) Activating a Patch Package by One Click

(3) Uninstalling a Patch Package

1.7.4 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** *slot-id* | **slot all**]

(3) Install the patch package by performing either of the following operations:

- Run the general patch command to install the patch package.

a Activate the installed patch temporarily.

install activate *package_name* [**slot** *slot-id* | **slot all**]

b Activate the patch permanently.

install commit [**slot** *slot-id* | **slot all**]

- Run the **patch** command to install the patch package.

a Activate the installed patch temporarily.

patch active [**slot** *slot-id* | **slot all**]

b Activate the patch permanently.

patch running [**slot** *slot-id* | **slot all**]

(4) Activate the patch permanently by one click.

patch auto-running [**slot** *slot-id* | **slot all**]

(5) (Optional) Restart the device for the patch to take effect.

reload

Run this command only after a cold patch is installed.

1.7.5 Activating a Patch Package by One Click

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

- To fix software bugs without upgrading the main program and perform temporary verification, activate the patch package temporarily by one click.
- To fix software bugs without upgrading the main program, activate the patch package permanently by one click.
- If you need to ignore the CPU and memory checks of the system when installing a patch, add the **ignore_cpu_mem** parameter to the one-click upgrade command. The CPU and memory waterlines are built-in by default in the system, and their values are both 85%.

Caution

The downloaded patch package cannot be renamed. The name of the patch package name is used as the operation keyword for the subsequent patch activation, deactivation, and uninstallation.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Activate the patch package by one click.

- Activate the patch package temporarily by one click.

  upgrade auto { *url* [**delay-time** *time-number*] | **download** { **ftp:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] | **https:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] | **sftp:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] | **tftp:**//*path* [**delay-time** *time-number*] [**vrf** *vrf-name*] } } [**force**]

- Activate the patch package permanently by one click.

  upgrade { *url* **patch-running** | **download** { **ftp:** //*path* **patch-running** [**vrf** *vrf-name*] | **https:** //*path* **patch-running** [**vrf** *vrf-name*] | **sftp:** //*path* **patch-running** [**vrf** *vrf-name*] | **tftp**: //path **patch-running** [**vrf** *vrf-name*] } } [**slot** *slot-id* | **slot all**] [**force**]

- Perform upgrade by one click to activate the patch package permanently.
  patch autoload *url* [**slot** *slot-id* | **slot all**] [**ignore_cpu_mem**]

1.7.6 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 one of the following commands to uninstall the patch package:

- Run the general patch command to uninstall a patch package.

  a Deactivate an activated patch.

  install deactivate *package_name* [**slot** *slot-id* | **slot all**]

  b Uninstall a patch.

  install remove *package_name* [**slot** *slot-id* | **slot all**]

- Run the **patch** command to uninstall a patch package.

  a Deactivate an activated patch.

patch deactivate *package_name* [**slot** *slot-id* | **slot all**]

b Uninstall a patch.

patch delete [**slot** *slot-id* | **slot all**]

1.7.7 Patch Auto-Sync

1. Overview

Configure the patch auto-sync policy for the distributed architecture system or the VSU system that consists of fixed devices.

2. Restrictions and Guidelines

When the patch auto-sync function is enabled, patches that meet the patch auto-sync rule are synchronized.

Patch auto-sync rules:

- All versions must come from the same rack package or Main package before patch auto-sync is performed.
- The patch installed on the active supervisor module or device 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 as follows: add, active, and running.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the patch auto-sync function.

install auto-sync { **disable** | **enable** }

The patch auto-sync function is enabled 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 **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 Software 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.
show upgrade auto-sync	Displays the auto-sync upgrade configuration on the device.
check version	Checks the version matching.
clear install storage [**slot** *slot-id* | **slot 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.
show patch auto-sync	Displays information about all patch packages that need to be automatically synchronized on the current device.
show cmpnt { **auto_db** | **new_list** | **upgrade_db** | { **begin** | **client** | **server** } { **backup** | **current** } { **all_log** | **error_log** | **major_log** | **msg_log** | **trace_log** } }	Debugs the patch.

1.9 Configuration Examples

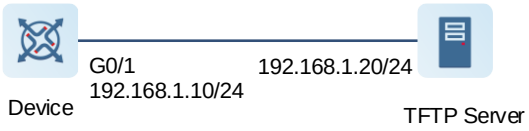
1.9.1 Configuring Subsystem Upgrade

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 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 Ethernet interface on the device so that the L3 route is reachable between the device and the TFTP server.
- Run the **upgrade download tftp:**//*path* command to upgrade the installation package file stored on the TFTP server.

4. Procedure

(1) Configure the Ethernet interface IP address on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.1.10 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# end
```

(2) Run the **upgrade download tftp:**//*path* command to upgrade the device.

```
Hostname# upgrade download tftp://192.168.1.20/main.bin 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
!!!
```

```
      Device type    : s5315
      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 192.168.1.20
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 1/0]
      Device type    : s5315
      Status         : ready
```

(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(S5315-24MG6XS-UP-E) By
Ruijie Networks
System start time      : 2024-05-17 06:26:02
System uptime          : 00:02:15:17
System hardware version : 1.00
System software version : S5315_RGOS 12.6(3)B0103
System patch number    : NA
System serial number   : G1TX6XX00892B
System boot version    : 1.1.16(Master) 1.1.16(Slave)
System rboot version   : 2.0.12
Module information:
  Slot 0 : S5315-24MG6XS-UP-E
    System uptime      : 00:02:15:17
    Hardware version   : 1.00
    Boot version       : 1.1.16(Master) 1.1.16(Slave)
    Rboot version      : 2.0.12
    Software version   : S5315_RGOS 12.6(3)B0103
```

```
   Serial number      : G1TX6XX00892B
   Serial number      : G1SK5RZ00175A
```

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 . Rack-type devices often have USB flash drives.
- The TFTP server is not enabled.

1.9.2 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/0424.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.

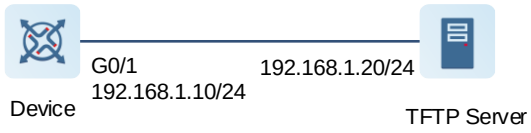
1.9.3 Installing a Patch Package

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

- Configure the L3 route reachable to the device.
- Copy the patch package to the device.
- Run the patch installation command.
- Activate a hot patch.
  - Activate a hot patch temporarily.
  - Activate a hot patch permanently.
- Configure patch auto-sync.

4. Procedure

(1) Configure the Ethernet interface IP address and default route on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.1.10 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# end
```

(2) Install a patch package.

```
Hostname# install add tftp://192.168.1.20/smu_rf_hot1002_0118.bin
Press Ctrl+C to quit
!
< The terminal is lock >
Operating, please wait for a moment.....
!!!!!     100%
```

```
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is unlock >
```

(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 lock >
Operating, please wait for a moment.......
!!!!!     100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is unlock >
```

  b Run the **install commit** command to activate the hot patch permanently.

```
Hostname# install commit
< The terminal is lock >
Operating, please wait for a moment...
!!!!!     100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is unlock >
```

- 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 lock >
Operating, please wait for a moment.......
!!!!!     100%
Patch operation finish!
Operate result information:
```

```
-------------------------------------
Slot          Result        Comment
1/0           Success       None
2/0           Success       None

< The terminal is unlock >
```

b Run the **patch running** command to activate the hot patch permanently.

```
Hostname# patch running
< The terminal is lock >
Operating, please wait for a moment...
!!!!!     100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot          Result        Comment
1/0           Success       None
2/0           Success       None

< The terminal is unlock >
```

(4) Configure automatic synchronization of the patch.

```
Hostname# configure
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# install auto-sync enable
```

5. Verification

Run the **show install** command to display information about the hot patches installed on the current device.

```
Hostname# show install
Install information:
 [Slot 1/0]
    Name                     State         Flag       Effective time        Package
    smu_rf_hot1002_0118.bin     running       Hot        2019-09-17 19:00:02

 [Slot 2/0]
    Name                     State         Flag       Effective time        Package
    smu_rf_hot1002_0118.bin     running       Hot        2019-09-17 19:00:02
```

Run the **show patch** command to display information about the hot patches installed on the current device.

```
Hostname# show patch
 [Slot 1/0]
    Patch package SP1 installed in the system, version:5.0.0.0
    ----------------------------------------
    Patch      : SP1.bin
    Status     : active
    Version    : 5.0.0.0
    Size       : 1770
```

```
    Install time: 2021-09-03 10:00:24
    Description : test SP1

[Slot 2/0]
    Patch package SP1 installed in the system, version:5.0.0.0
    ----------------------------------------
    Patch      : SP1.bin
    Status     : active
    Version    : 5.0.0.0
    Size       : 1770
    Install time: 2021-09-03 10:00:24
    Description : test SP1
```

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.

1.9.4 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 lock >
Operating, please wait for a moment.......
!        100%
Patch operation finish!
Operate result information:
-----------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is lock >
```

b Run the **install remove** command to uninstall the patch.

```
Hostname#install remove smu_rf_hot1002_0118.bin
< The terminal is lock >
Operating, please wait for a moment...
!        100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is lock >
```

- Run the **patch** command to uninstall a patch.

a Run the **patch deactive** command to deactivate the patch.

```
Hostname# patch deactive
< The terminal is lock >
Operating, please wait for a moment.......
!        100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is lock >
```

b Run the **patch delete** command to uninstall the patch.

```
Hostname# patch delete
< The terminal is lock >
Operating, please wait for a moment...
!        100%
Patch operation finish!
Operate result information:
-------------------------------------
Slot         Result       Comment
1/0          Success      None
2/0          Success      None

< The terminal is lock >
```

4. Verification

Run the **show install** command to display the patch uninstallation result.

```
Hostname#show install
```

```
Install information:
 [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 patch package installed in the systemInstall information]

 [Slot 2/0]
    [No patch package installed in the systemInstall information]
```

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 specific requirement.

(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 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 License Management 1

1.1 Introduction 1

1.1.1 License Management Overview 1

1.1.2 Principles 1

1.2 Configuration Task Summary 3

1.3 Configuring License Management 3

1.3.1 Overview 3

1.3.2 Installing License File 4

1.3.3 Backing Up License File 5

1.3.4 Configuring Grace Period Warning 5

1.3.5 Updating License File 6

1.3.6 Uninstalling License 6

1.3.7 Unbinding License 7

1.4 Monitoring 7

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. A user can use the general and extension functions of the Ruijie General Operating System (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.

Specification

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.

Licensing for modular devices takes effect on a single device basis. In a VSU environment, the entire VSU system is licensed to use a feature only after all devices obtain the license for that feature. Licensing or delicensing takes effect only after the devices are restarted.

- 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.

- Multi-instance license

  Multiple license files can be installed for the same feature on a device.

- 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.

- 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.
- Install the license file.
  - If you run the **license install** command in the VSU environment, the license file is installed only on the local device or supervisor module.
  - If you run the **license auto-install** command in the VSU environment, the license file is automatically installed on the matched device.
  - In a VSU environment, you can run the **license auto-install** command to automatically match the device for installing the license file. In a non-VSU environment, the **license auto-install** command has the same function as the **license install** commands.

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. Perform either of the following operations as required.

- Install a license in the system.

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

- Automatically install a license on the matched device in the VSU system.

  license auto-install { **flash:** | **usb0:** } *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.

- Back up all perpetual license files in the system.

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

- Back up a license file or the license file specified by the feature name.

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

No license file is backed up by default.

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 for reminding the user of the expiration of a license.

license grace-period *filename time*

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 the device is 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.

- Uninstall a license in the system.

  license uninstall *license* [*filename*]

- Uninstall a license from a specified device in a VSU.

  license auto-uninstall *device-id 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.
- The function of the **license auto-unbind** command in a non-VSU environment is the same as that of the **license unbind** command.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Unbind a license from the system. Perform either of the following operations as required.

- Unbind a license from the system.
  license unbind *pak*
- Unbind a license from a specified device in the VSU system.
  license auto-unbind *device-id 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.

Command	Purpose
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.

Device Management Configuration

1. Configuring NTP
2. Configuring SNTP
3. Configuring Time Range
4. Configuring Process Restarting
5. Configuring Supervisor Module Redundancy
6. Configuring Module Hot Swapping
7. Configuring Forwarding Path Monitoring
8. Configuring Intelligent Hardware Monitoring
9. Configuring Intelligent Component Monitoring

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 4
1.2 Restrictions and Guidelines 4
1.3 Configuration Task Summary 4
1.4 Configuring NTP Security Authentication 5
1.4.1 Overview 5
1.4.2 Restrictions and Guidelines 5
1.4.3 Procedure 5
1.5 Configuring Basic Functions of NTP 6
1.5.1 Restrictions and Guidelines 6
1.5.2 Configuration Tasks 6
1.5.3 Configuring NTP in Client/Server Mode 6
1.5.4 Configuring NTP in Peer Mode 7
1.5.5 Configuring NTP in Broadcast Mode 8
1.6 Configuring NTP-Related Parameters 8
1.6.1 Procedure 8
1.7 Configuring NTP Access Control 9
1.7.1 Overview 9
1.7.2 Restrictions and Guidelines 9

1.7.3 Procedure.....10
1.8 Monitoring.....10
1.9 Configuration Examples.....11
1.9.1 Configuring the Local Clock Reference Mode of NTP.....11
1.9.2 Configuring the External Clock Reference Mode of NTP.....12
1.9.3 Configuring NTP Security Authentication.....15
1.9.4 Configuring NTP Access Control Rights.....17
1.9.5 Configuring the NTP Broadcast Mode.....19
1.9.6 Configuring the NTP Peer Mode.....20

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. When a device is used as a server, it supports only the unicast server mode. It also supports the peer mode and broadcast mode.

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.

- Active peer

  The active peer periodically sends a synchronization packet in which **Mode** is set to **1** to the passive peer, without considering reachability and stratum of its peer. The host running in this mode can either provide synchronization information to the peer, or synchronize the local clock based on the peer's time information.

- Passive peer

  The passive peer receives a synchronization packet from the active peer, and responds with a packet in which **Mode** is set to **2**. The host running in the passive peer mode can either provide synchronization information to the peer, or synchronize the local clock based on the peer's time information.

- Broadcast server

  In broadcast mode, the server periodically sends a clock synchronization packet in which **Mode** is set to **5** to the broadcast address 255.255.255.255, without considering reachability and stratum of its peer. The host running in broadcast mode is usually a time server running high-speed broadcast media in the network. It provides synchronization information to all peers, but does not modify its own clock.

- Broadcast client

The client listens to the clock synchronization packet from the server. After the client receives the first clock synchronization packet, it exchanges an NTP packet in which **Mode** is **3** (client mode) or **4** (server mode) with the server. That is, the client enables server/client mode for a short period of time to exchange messages with the remote server to obtain the network delay between the client and the server. The client then resumes the broadcast mode, continues to listen to the arrival of the clock synchronization packet, and synchronizes the local clock again based on the incoming clock synchronization packet.

- **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**.

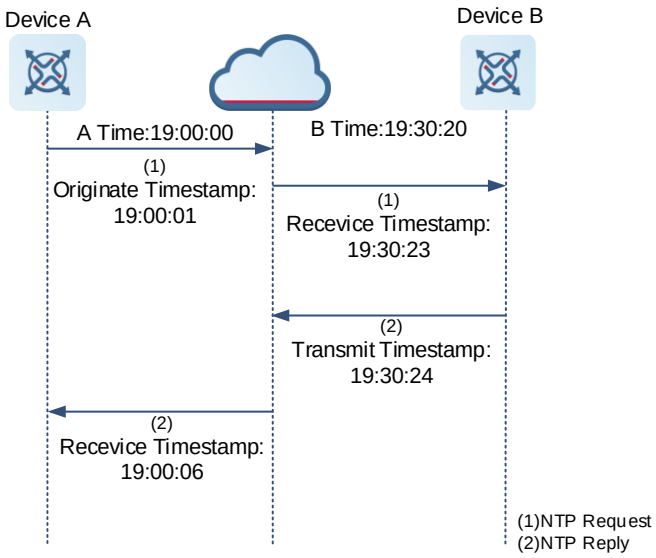
(3) After a network delay of 2s, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

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.
- Peer mode
  - The peer mode runs at a lower stratum in the synchronization subnet. In this mode, the active peer and passive peer can synchronize time with each other. The passive peer needs to run the **ntp passive enable** command to enable the function of receiving packets in peer mode to eventually implement time synchronization.
  - In peer mode, a peer with a higher stratum provides time synchronization for a peer with a lower stratum.
- Broadcast mode
  - When the IP address of the server or peer cannot be determined, or too many devices in the network need time synchronization, the broadcast mode can be used to achieve time synchronization.
  - You need to configure related commands on both the server and the client. Only the client can synchronize time with the server.

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 Layer 3 Ethernet interfaces or link aggregations 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 Basic Functions of NTP

  a Configuring NTP in Client/Server Mode

  b (Optional) Configuring NTP in Peer Mode

  c (Optional) Configuring NTP in Broadcast 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* [**0** | **7**]

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 [vrf *vrf-name*] { *ipv4-address* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } *[* **key** *keyid* | **prefer** | **source** *interface-type interface-number* | **version** *version] **

By default, no authentication key ID is configured for an external reference clock source.

1.5 Configuring Basic Functions of NTP

1.5.1 Restrictions and Guidelines

- When configuring the NTP server, you must specify at least one external reference clock source. A maximum of 20 different external reference clock sources can be configured.
- If it is necessary to configure an NTP key, you must configure NTP security authentication before configuring the NTP server. A device that acts as a client supports interaction with up to 20 NTP servers. You can configure an authentication key for each server (after configuring global authentication and the related key) to initiate encrypted communication with the servers.
- The default version of NTP for communicating with a server is NTP version 4. In addition, you can configure the source interface for transmitting NTP packets and specify that the NTP packets from a corresponding server can be received only on the transmitting interface.
- After a local clock is configured as the master clock (especially when a clock with a lower stratum is specified), the system does not synchronize with a clock source with a higher stratum, and therefore a real effective clock source may be overwritten. If this function is used for multiple devices in a network, the clock difference between the devices may cause unstable time synchronization of the network.
- Before a local clock is configured as the master clock, if the system never synchronizes time with an external clock source, you may need to manually calibrate the system clock to ensure that there is no excessive difference. For details about how to manually calibrate the system clock, refer to the basic management section in the Basic Configuration Commands.
- By default, if NTP works in client/server mode, after the NTP device synchronizes time from an external reliable clock source, the device acts as the time server to provide the time synchronization service for other devices. If you configure an NTP device only as a client, run the **ntp service disable** command to disable the external time synchronization service provided by NTP. After this command is configured, an external device cannot synchronize time from this NTP device.

1.5.2 Configuration Tasks

(1) Configuring NTP in Client/Server Mode

(2) (Optional) Configuring NTP in Peer Mode

(3) (Optional) Configuring NTP in Broadcast Mode

1.5.3 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 [vrf *vrf-name*] { *ipv4-address* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } *[* **key** *keyid* | **prefer** | **source** *interface-type interface-number* | **version** *version] **

1.5.4 Configuring NTP in Peer Mode

1. Overview

This section describes how to configure NTP in peer mode. Assume that device A has synchronized time with the server, and device B has not synchronized time with the server. If device A acts as the active peer of device B, device B synchronizes time with device A. Alternatively, if device B acts as the active peer of device A, device B synchronizes time with device B.

2. Restrictions and Guidelines

- When configuring the peer mode, you must configure the **ntp passive enable** command on the passive peer to enable the function of receiving packets in peer mode.
- A client can concurrently interact with up to 20 peers.
- If you need to configure an authentication key, configure NTP security authentication before you can configure an authentication key for each peer to initiate encrypted communication with the peer.

  NTP version 4 supports communication with peers. You can also configure the source interface for transmitting NTP packets and specify that the NTP packets from a peer can be received only on the transmitting interface.
- At least one of the clocks of the active peer and the passive peer must be in synchronized state. Otherwise, they cannot synchronize time.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the NTP peer mode. Configure at least one of the following tasks.

- Configure the NTP peer mode.

  ntp peer [**vrf** *vrf-name*] { *ipv4-address* | *peer-name* | *ipv6-address* | **ip** *domain* | **ipv6** *domain* } [**key** *keyid*] [**prefer**] [**source** *interface-type interface-number*] [**version** *version*]

  No NTP peer mode is configured by default.
- Configure the NTP passive peer.

  ntp passive enable

  No NTP passive peer is configured by default.

1.5.5 Configuring NTP in Broadcast Mode

1. Overview

This section describes how to configure NTP in broadcast mode. After the broadcast server and broadcast client are enabled, the server periodically sends broadcast packets to 255.255.255.255, and the broadcast client receives the broadcast packets and synchronizes time accordingly.

2. Restrictions and Guidelines

- If the broadcast client mode is disabled on the device, time synchronization is not performed.
- The packet sending period is the maximum polling time. Plus the algorithm selection, the first synchronization time is longer.

3. Prerequisites

Before configuring NTP in broadcast mode, you need to configure a clock reference source for the broadcast server so that the server's clock is in synchronized state. Otherwise, the broadcast client cannot synchronize time from the broadcast server.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Configure NTP in broadcast mode. Configure at least one of the following tasks.

- Configure an NTP broadcast server.

  ntp broadcast-server [**key** *key-id*] [**version** *version*]

  The broadcast server is disabled on an interface by default.

- Configure an NTP broadcast client.

  ntp broadcast-client

  The broadcast client is disabled on an interface 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *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** { *acl-name* | *acl-number* } [**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** { *acl-name* | *acl-number* } [**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** | **query-only** | **serve** | **serve-only** } { *acl-name* | *acl-number* } [**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 peer	Displays the NTP peer list.
show ntp broadcast-server	Displays the NTP broadcast server list.
debug ntp	Debugs the DNS function.
no debug ntp	Disables the debugging function.

1.9 Configuration Examples

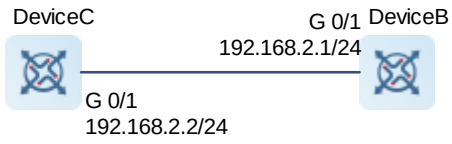
1.9.1 Configuring the Local Clock Reference Mode of NTP

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
```

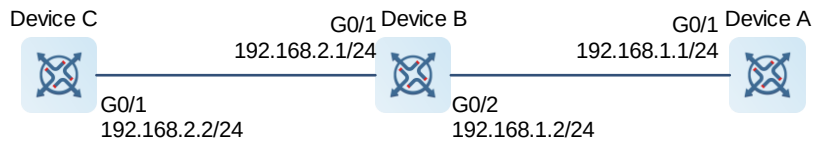
1.9.2 Configuring the External Clock Reference Mode of NTP

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 Device B
!
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
```

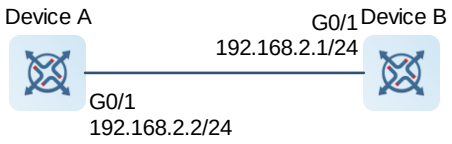
1.9.3 Configuring NTP Security Authentication

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
```

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".

```
Device A(config)# ntp master
Device A(config)# ntp authenticate
Device A(config)# ntp authentication-key 1 md5 abcd
```

```
Device A(config)# ntp trusted-key 1
```

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 key 1
```

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
    ntp authentication-key 1 md5 abcd
    ntp authenticate
ntp trusted-key 1
!
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 key 1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
end
```

1.9.4 Configuring NTP Access Control Rights

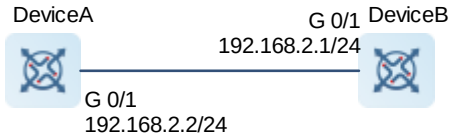
1. Requirements

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
```

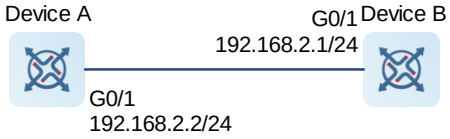
1.9.5 Configuring the NTP Broadcast Mode

1. Requirements

Use device A as the broadcast server to provide the time synchronization service for device B.

2. Topology

Figure 1-6 Topology for NTP Broadcast Mode



3. Notes

- Configure the local clock of Device A as the NTP reference source, and Device A as the NTP broadcast server.
- Configure device B as the NTP broadcast client to synchronize time from Device A.

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
```

Configure the local clock of device A as the NTP reference clock source.

```
DevcieA(config)# ntp master
```

Configure device A as the NTP broadcast server.

```
DevcieA(config)# interface gigabitEthernet 0/1
DevcieA(config-if-GigabitEthernet 0/1)# ntp broadcast-server
```

Configure device B as the NTP broadcast client.

```
DevcieB(config-if-GigabitEthernet 0/1)# ntp broadcast-client
```

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
 ntp broadcast-server
 ip address 192.168.2.2 255.255.255.0
!
ntp master
!
end
```

Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ntp broadcast-client
 ip address 192.168.2.1 255.255.255.0
!
end
```

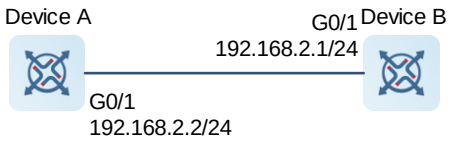
1.9.6 Configuring the NTP Peer Mode

1. Requirements

A time server, device A, exists in the network, and device B needs to synchronize time from device A. Configure device A as the passive peer and device B as the active peer.

2. Topology

Figure 1-7 Topology for NTP Peer Mode



3. Notes

- Configure device A as the passive peer.
- Configure device B as the active peer.

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 the local clock of device A as the NTP reference clock source.

```
DeviceA(config)# ntp master
```

Configure device A as the passive peer.

```
DeviceA(config)# ntp passive enable
```

Configure device B as the active peer to synchronize time from device A.

```
DeviceB(config)# ntp peer 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
 ntp broadcast-server
 ip address 192.168.2.2 255.255.255.0
!
ntp passive enable
ntp master
!
end
```

Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ntp broadcast-client
 ip address 192.168.2.1 255.255.255.0
!
ntp peer 192.168.2.2
!
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 Configuring 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.

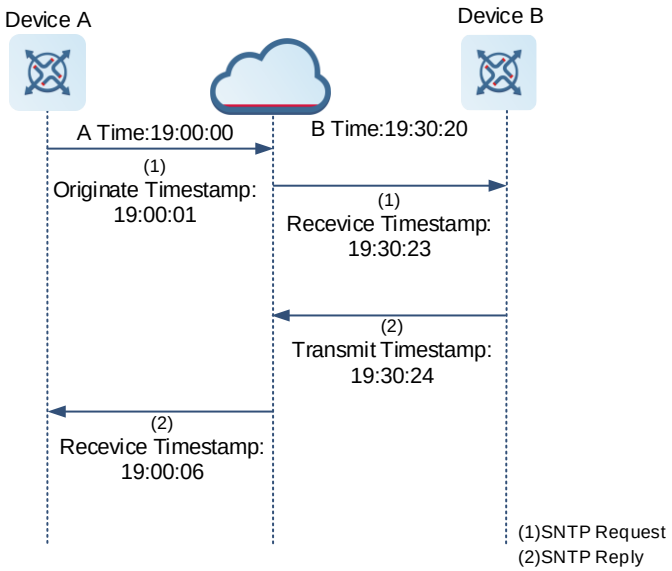
(4) After a network delay of 2s, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

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 { *domain* | *ipv4-address* } [**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

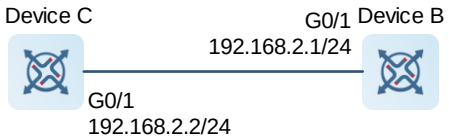
1.5.1 Configuring Basic Functions of SNTP

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 Basic SNTP 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 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 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

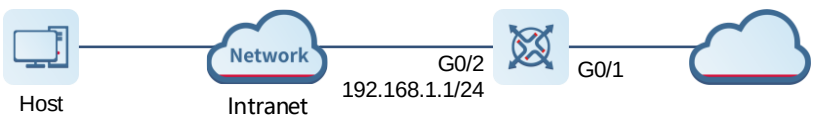
1.4.1 Configuring Basic Features of Time Range

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 0/2.

```
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# 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 0/2.
```

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 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 Restarting a Process of the Member Device in a Specified Slot on a Specified Device 2

1.5 Starting a Process of the Member Device in a Specified Slot on a Specified Device 2

1.6 Stopping a Process of the Member Device in a Specified Slot on a Specified Device 2

1.7 Displaying Processes that can Be Restarted on the Member Device in a Specified Slot on a Specified Device 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 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**

1.5 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**

1.6 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**

1.7 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**

Contents

1 Configuring Supervisor Module Redundancy 1
1.1 Introduction 1
1.1.1 Overview 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 Active/Standby Switchover 3
1.4.3 Configuring an Automatic Synchronization Period 4
1.4.4 Resetting Devices 5
1.4.5 Disabling Active/Standby Switchover 5
1.5 Configuring Automatic Synchronization Mode 5
1.5.1 Overview 5
1.5.2 Procedure 6
1.6 Configuring an Active/Standby Switchover Timeout Period 6
1.6.1 Overview 6
1.6.2 Restrictions and Guidelines 6
1.6.3 Procedure 6
1.7 Monitoring 6

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.

Principles

1. Basic Concepts

- Global active/standby

  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 active device, another as the global standby device..

- Prerequisites for redundancy of supervisor modules

  The SM redundancy 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 active device and the standby device to ensure their state consistency. Before this process, the SM redundancy does not fully play its role.

- Redundancy state of supervisor modules

  During active-standby backup, the active device has three states as follows:

  - alone, namely alone state. In this state, only one device is running in the system or active/standby switchover is not completed and no redundancy is created between the new active device and the new standby device.
  - batch, namely batch backup state. Redundancy is created between the active device and the standby device and batch backup is in progress.
  - realtime state, namely real-time backup state. Upon batch backup, the active and standby devices are in this state. Real-time backup is performed between the active device and the standby device. Only in this state manual switchover is allowed.

2. Election of Active and Standby Devices

- Automatic Election

  A VSU is composed of at least an active device and a standby device. When more than two devices exist in a VSU, devices except the active and standby 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 priorities of the rules for selecting the standby device are 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 the active/standby role, even if the device has a higher priority than the active and standby devices in the VSU.
- The startup sequences 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 VSU.

- Manual Selection

  In VSU mode, you can manually perform active/standby switchover to promote the global standby device to the global active device. If only two member devices exist in the VSU, the original global active device is reset and becomes the new global standby device. If more than two member devices exist in the VSU, a global candidate device is promoted to the new global standby device, and the original global active device is reset and becomes a global candidate device.

3. Active/Standby Information Synchronization

- Status Synchronization

  The active device synchronizes its running status to the standby device in real time so that the standby device can take over the function of the active device at any time without noticeable changes.

- Configuration Synchronization

  During device running, two types of system configuration files exist: One is the configuration file dynamically generated during running, which changes with the service configuration, and is called running-config. The other is the system configuration file imported when the device is started, which is called startup-config. You can synchronize the running-config file with the startup-config file using the **write** command writes the running-config to startup-config. Alternatively, use the **copy** command to copy the content of the running-config file to the startup-config file.

  For functions that are not directly related to uninterrupted forwarding, the synchronization of system configuration files ensures the consistency of user configurations during switchover.

  With VSU member redundancy, the active device synchronizes the startup-config and running-config configuration files to the standby device and all candidate devices. Configuration files are synchronized in the following operations:

  - When you exit from the global configuration mode to privileged EXEC mode, the running-config file is synchronized.

- When you use the **write** command **to** save configurations or the **copy** command to copy configurations, the startup-config file is synchronized.

Note

The configuration delivered through SNMP cannot be automatically synchronized to the startup-config file. You can run the **write** or **copy** command to synchronize the running-config file.

- 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 active-standby backup 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.

- Configuring Manual Active/Standby Switchover
- Configuring an Automatic Synchronization Period
- Resetting Devices
- Disabling Active/Standby Switchover
- Configuring Automatic Synchronization Mode
- Configuring an Active/Standby Switchover Timeout Period

1.4 Configuring RDND

1.4.1 Overview

- The device automatically selects the active and standby SMs based on the current system, or users do so manually.
- In the SM redundancy environment, the active SM synchronizes status information and configuration files to the standby SM in real time.

1.4.2 Configuring Manual Active/Standby Switchover

1. Overview

If there are more than two devices in the system, the devices can automatically select the active and standby devices based on the current system status, or the user can manually select the active and standby devices. After manual active/standby switchover is configured, the standby device becomes the active device, and a new standby device is elected from the candidate devices. After the original active device is reset, it becomes a candidate device.

2. Restrictions and Guidelines

- To ensure smooth data forwarding during switchover, perform batch synchrhonization performed between the active supervisor module and the standby supervisor module so that the two modules are in the same state. That is, manual switchover is allowed only when the redundancy of SMs is in the real-time backup state. In addition, manual active/standby switchover is temporarily disabled by service modules during synchronization to ensure that configuration files are completely synchronized. Therefore, the following conditions must be met for the manual switchover:
  - The operation is performed on the active device and a standby device exists.
  - The hot backup in the system is in the real-time state.
  - The active/standby switchover in the system is not temporarily disabled by service modules.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Perform an active/standby switchover.

redundancy forceswitch

1.4.3 Configuring an Automatic Synchronization Period

1. Overview

By configuring the automatic synchronization period, you can adjust the synchronization period of the configuration files (**startup-config** and **running-config**) for the active SM or device.

Restrictions and Guidelines

It is recommended that a short synchronization period be configured so that the active 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 standby device due to the failure of the active device.

2. 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 Devices

1. Overview

Resetting only the standby SM does not affect data forwarding. During the resetting of the standby SM, forwarding is not interrupted or user session information is not lost.

You can run the **redundancy reload shelf** command in standalone mode to reset the entire device. In VSU mode, the device with the specified ID is reset. If the global active device is specified to be reset with two or more devices in the system, the system performs an active/standby switchover.

2. Restrictions and Guidelines

In VSU mode, if the SMs of the system are not in the real-time backup state, resetting the device where the global active SM resides will cause the whole VSU system to reset.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Reset a device.

redundancy reload { **peer** | **shelf** [*switch-id*] }

1.4.5 Disabling Active/Standby Switchover

1. Overview

This section describes how to disable forcible active/standby switchover.

2. Restrictions and Guidelines

After the configuration takes effect, the function of the **redundancy forceswitch** command is disabled.

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) Disable forcible active/standby switchover.

switch-disable

Forcible active/standby switchover is enabled by default.

1.5 Configuring Automatic Synchronization Mode

1.5.1 Overview

By configuring the hot standby automatic synchronization mode, you can specify the configuration files to be synchronized by the active SM. The configuration files include the running-config and startup-config files.

1.5.2 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 the automatic synchronization mode of hot standby.

auto-sync { **running-coinfig** | **standard** | **startup-config** }

The automatic synchronous mode is standard by default.

1.6 Configuring an Active/Standby Switchover Timeout Period

1.6.1 Overview

You can modify the active/standby switchover timeout period through configuration.

1.6.2 Restrictions and Guidelines

- You are advised to use the default value unless otherwise specified.

1.6.3 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 the active/standby switchover timeout period.

switchover timeout *timeout-value*

The timeout period for active/standby switchover is 4,000 ms 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 rdnd { **clients** | **dbinfo** | **disable** | **elements** | **inter-connection** | **keyentity** | **logs** | **netconf-state** | **pairs** | **problems** | **status** [**details**] | **switchover** | **sync** }	Debugs the hot standby information.
show redundancy auto-sync	Displays the automatic synchronization mode of hot standby.
show redundancy states	Displays the current redundancy status of device
show redundancy switchtimeout	Displays the timeout period for the active/backup switchover of hot standby.

Contents

1 Configuring Module Hot Swapping 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Working Principle 1

1.2 Configuration Task Summary 1

1.3 Clearing and Modifying Module/Device Configurations 2

1.3.1 Overview 2

1.3.2 Procedure 2

1.4 Setting the Application Level of a Device 2

1.4.1 Overview 2

1.4.2 Procedure 2

1.5 Monitoring 3

1 Configuring Module Hot Swapping

1.1 Introduction

1.1.1 Overview

Module hot swapping is a maintenance function provided by devices. 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 on devices.

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.

2. Card Pre-installation

The card pre-installation is supported. That is, after the installed card is removed, if you save the configuration and restart the device, the configuration of the card is not lost.

3. Application Level of a Device

In global configuration mode, run the **device-level** command to set the application level for a device, which can be the core layer, convergence layer, or access layer. By default, a device obtains its application level from the xml file that describes the device. When the **show running-config** command is run under the default configuration, the application level of the device is not displayed. The **show device-level** command can be run to display the application level of the current device. When no configuration exists, "unknown" is displayed.

1.2 Configuration Task Summary

Note

The module hot swapping function is automatically implemented and no manual configuration is required.

The module hot swapping configuration includes the following tasks:

- Clearing and Modifying Module/Device Configurations
- Setting the Application Level of a Device

1.3 Clearing and Modifying Module/Device Configurations

1.3.1 Overview

In different circumstances, different configurations need to be cleared. The specific application scenarios are described as follows:

- 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 device. 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.

1.3.2 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.

1.4 Setting the Application Level of a Device

1.4.1 Overview

This section describes how to set the application level for a device so that the administrator can intuitively learn the network layer to which the device belongs. Configurable application levels include the core layer, convergence layer, and access layer.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the application level of the device.

device-level { **core** | **collect** | **access** }

The application level of a device is obtained from the XML file by default.

1.5 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 devices	Displays the device information.
show version module detail [*slot-number*] **show version module detail** [*device-id/slot-number*] (in VSU mode)	Displays the details of a module.
show version slots [*slot-number*] **show version slots** [*device-id/slot-number*] (in VSU mode)	Displays the online status of a module.
show cpld-fpga version	Displays the hardware version number of the 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.
show vsd-summary	Displays the VSD summary.
show web-api custom_info	Displays customization information provided for the web.
show web-api version	Displays the version information provided for the web.

Contents

1 Configuring Backplane Interface Monitoring 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Configuration Task Summary 2

1.3 Configuring Backplane Interface Exception Alarm 2

1.3.1 Overview 2

1.3.2 Restrictions and Guidelines 3

1.3.3 Configuration Tasks 3

1.3.4 Configuring the Maximum Number of Exception Alarm Syslogs 3

1.3.5 Configuring Polling Periods 3

1.3.6 Configuring Alarms for CRC Errors 4

1.3.7 Configuring Alarms for Backplane Interface Jitters 4

1.3.8 Configuring Alarms for Abnormal Backplane Interface Disabling 4

1.4 Configuring Automatic Isolation of Backplane Interfaces 5

1.4.1 Overview 5

1.4.2 Restrictions and Guidelines 5

1.4.3 Configuration Tasks 5

1.4.4 Configuring Automatic Isolation 5

1.4.5 Configuring the Number of Polling Periods for Triggering Isolation 5

1.5 Configuring Isolated Backplane Interface Restoration 6

1.5.1 Overview 6

1.5.2 Restrictions and Guidelines 6

1.5.3 Configuration Tasks 6

1.5.4 Disabling Automatic Isolation 6

1.5.5 Restoring an Isolated Backplane Interface 6

1.6 Monitoring 7

1.7 Configuration Examples 7

1.7.1 Configuring Backplane Interface Exception Alarms and Automatic Isolation 7

1 Configuring Backplane Interface Monitoring

1.1 Introduction

1.1.1 Overview

This function supports status query, alarm reporting, automatic isolation, and manual restoration of backplane interfaces on box-type devices. When a backplane interface on a board card is abnormal (for example, incorrect frames due to chip pin damage, abnormal disabling and jitter of a backplane interface), backplane interface monitoring notifies users of the abnormal backplane interface and automatically isolates the interface according to the configured isolation detection rules to prevent packet loss or other errors. Isolation detection rules are configured by default before delivery, and users can change some configurations. Backplane interface monitoring also allows users to query the physical status of backplane interfaces.

1.1.2 Principles

1. Basic Concepts

- Backplane

  A backplane is a framework that is connected with different board cards (generally line cards and FE cards) of a box-type device.

- Backplane interface

  A backplane interface is used by a board card (supervisor engine, FE card, or line card) to be connected with another board card through the backplane.

- Polling period

  Backplane interface monitoring checks errors and jitters of a backplane interface in polling mode to determine the backplane interface status. If an exception of a backplane interface reaches the preset threshold within a polling period, an alarm is generated. The maximum number of alarm logs configured by users or configured by default before delivery takes effect only within one polling period. Users can change the default configuration.

- Polling periods for automatic isolation

  When the automatic isolation function is enabled, backplane interface monitoring isolates a backplane interface only when the number of accumulated exceptions on the backplane interface exceeds the specified number of exceptions in specified number of polling periods. This prevents a normal backplane interface from being isolated due to misjudgment. Users are allowed to configure the polling threshold. Generally, a greater polling threshold indicates a smaller misjudgment probability.

2. Exception Alarm

During normal system running, backplane interface monitoring monitors the status of all backplane interfaces. If an exception is found, an alarm syslog is printed.

This function checks the backplane interface status and statistics in polling mode periodically. If a cyclic redundancy check (CRC) error, jitter, abnormal disabling is found, an alarm syslog is printed.

Alarm syslogs for backplane interface exceptions start with "%FABRIC-4".

3. Automatic Isolation of Abnormal Backplane Interfaces

When the automatic isolation function of backplane interfaces is enabled, backplane interface monitoring actively isolates abnormal backplane interfaces to prevent them from affecting the service traffic.

Backplane interface monitoring isolates and disables backplane interfaces with consecutive CRC errors or jitters to prevent traffic from being forwarded through such interfaces. To prevent misjudgment, a backplane interface is isolated only when the backplane interface is abnormal in *N* consecutive polling periods.

4. Restoration of Isolated Backplane Interfaces

Backplane interface monitoring automatically isolates backplane interfaces with consecutive CRC errors or jitters. Users can restore the isolated backplane interfaces. A restored backplane interface is deleted from the isolation list, and continues to undergo exception detection. To restore an isolated backplane interface, you can disable the exception detection function, power off the board card to which the backplane interface belongs or the peer board card, or configure the isolated backplane interface restoration.

1.2 Configuration Task Summary

All of the following tasks are optional. Select them based on your actual requirements.

- Configuring Backplane Interface Exception Alarm
  - Configuring the Maximum Number of Exception Alarm Syslogs
  - Configuring Polling Periods
  - Configuring Alarms for CRC Errors
  - Configuring Alarms for Backplane Interface Jitters
  - Configuring Alarms for Abnormal Backplane Interface Disabling
- Configuring Automatic Isolation of Backplane Interfaces
  - Configuring Automatic Isolation
  - Configuring the Number of Polling Periods for Triggering Isolation
- Configuring Isolated Backplane Interface Restoration
  - Disabling Automatic Isolation
  - Restoring an Isolated Backplane Interface

1.3 Configuring Backplane Interface Exception Alarm

1.3.1 Overview

During normal system running, backplane interface monitoring monitors the status of all backplane interfaces at any time. If an exception is found, an alarm syslog is printed. Users can configure the function of backplane interface exception alarm to:

- Change the maximum number of alarm syslogs that are printed in a polling period.
- Change the enabling\disabling status of different types of alarm syslogs. Supported exception alarm types include CRC errors, jitters, and abnormal disabling of backplane interfaces.
- Configure the polling period for checking backplane interface exceptions.

1.3.2 Restrictions and Guidelines

The configured detection rules for backplane interface exception alarm are effective for all board cards in a cluster.

1.3.3 Configuration Tasks

All of the following tasks are optional. Select them based on your actual requirements.

- Configuring the Maximum Number of Exception Alarm Syslogs
- Configuring Polling Periods
- Configuring Alarms for CRC Errors
- Configuring Alarms for Backplane Interface Jitters
- Configuring Alarms for Abnormal Backplane Interface Disabling

1.3.4 Configuring the Maximum Number of Exception Alarm Syslogs

1. Overview

By configuring the maximum number of exception alarm syslogs, users can, according to their actual requirements, adjust the maximum number of backplane interface exception alarm syslogs that are displayed in a polling period.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of exception alarm syslogs.

fabric-interface warning limit *limit-number*

The maximum number of alarm logs for backplane interface exceptions that are displayed is 30 by default.

1.3.5 Configuring Polling Periods

1. Overview

By configuring the polling period for checking backplane interface exceptions, users can control the time for automatic isolation of abnormal backplane interfaces.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the time of a polling period.

fabric-interface polling-period *interval*

The polling period for backplane interface detection is 60 seconds by default.

1.3.6 Configuring Alarms for CRC Errors

1. Overview

When a CRC error occurs, an alarm is generated.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the alarm switch for CRC errors.

fabric-interface warning crc-error { **on** | **off** }

The alarm function for backplane interface CRC errors is enabled by default.

1.3.7 Configuring Alarms for Backplane Interface Jitters

1. Overview

When backplane interface jitter occurs, an alarm is generated.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure alarms for backplane interface jitters.

fabric-interface warning jitter { **on** | **off** }

The alarm function for backplane interface jitters is enabled by default.

1.3.8 Configuring Alarms for Abnormal Backplane Interface Disabling

1. Overview

When a backplane interface is disabled abnormally, an alarm is generated.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure alarms for abnormal backplane interface disabling.

fabric-interface warning abnormal-down { **on** | **off** }

The alarm function for abnormal backplane interface disabling is enabled by default.

1.4 Configuring Automatic Isolation of Backplane Interfaces

1.4.1 Overview

When the automatic isolation function of backplane interfaces is enabled, backplane interface monitoring actively isolates abnormal backplane interfaces to prevent them from affecting the service traffic. The automatic isolation function of abnormal backplane interfaces allows users to control enabling and disabling of automatic backplane interface isolation and change the polling period threshold for triggering automatic isolation.

1.4.2 Restrictions and Guidelines

After the function of automatic backplane interface isolation is configured, the isolation rules are effective for all chassis in a cluster.

1.4.3 Configuration Tasks

All of the following tasks are optional. Select them based on your actual requirements.

- Configuring Automatic Isolation
- Configuring the Number of Polling Periods for Triggering Isolation

1.4.4 Configuring Automatic Isolation

1. Overview

This section describes how to configure the automatic isolation function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the automatic isolation function.

fabric-interface isolate { **on** | **off** }

The automatic isolation function of abnormal backplane interfaces is disabled by default.

1.4.5 Configuring the Number of Polling Periods for Triggering Isolation

1. Overview

This section describes how to configure the polling period threshold for triggering automatic isolation of a backplane interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the number of polling periods for triggering isolation.

fabric-interface isolate polling-cnt *count-number*

The number of polling periods for triggering isolation conditions of backplane interfaces is 3 by default.

1.5 Configuring Isolated Backplane Interface Restoration

1.5.1 Overview

Backplane interface monitoring automatically isolates backplane interfaces with consecutive CRC errors or jitters. The function of isolated backplane interface restoration allows users to delete an isolated backplane interface from the isolation list. This backplane interface is restored to normal, and continues to undergone exception detection.

1.5.2 Restrictions and Guidelines

To restore an isolated backplane interface, you can disable the exception detection function, power off the board card to which the backplane interface belongs or the peer board card, or configure isolated backplane interface restoration.

1.5.3 Configuration Tasks

All of the following tasks are optional. Select them based on your actual requirements.

- Disabling Automatic Isolation
- Restoring an Isolated Backplane Interface

1.5.4 Disabling Automatic Isolation

1. Overview

This section describes how to disable the automatic isolation function.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable the automatic isolation function.

fabric-interface isolate off

The automatic isolation function of backplane interface is disabled by default.

1.5.5 Restoring an Isolated Backplane Interface

1. Overview

This section describes how to configure the number of polling periods for restoring an isolated backplane interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Restore an isolated backplane interface.

- Standalone device

fabric-interface isolate recovery port *port-id*

- Virtual Switching Unit (VSU) device

fabric-interface isolate recovery device *device-id* **port** *port-id*

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
VSU mode: **show fabric-interface connectivity** [**device** *device-id* [**port** *port-id*]] Standalone mode: **show fabric-interface connectivity** [**port** *port-id*]	Displays the backplane interface connection topology.
show fabric-interface isolate info	Displays the isolated backplane interfaces.
show fabric-interface monitor plan	Displays the current monitoring configurations.
VSU mode: **show fabric-interface status** [**device** *device-id* [**port** *port-id*]] Standalone mode: **show fabric-interface status** [**port** *port-id*]	Displays the physical and isolation status information of the backplane interface.
VSU mode: **show fabric-interface** status link-**history** [**device** *device-id* [**port** *port-id*]] Standalone mode: **show fabric-interface status link-history** [**port** *port-id*]	Displays the last 10 changes of the physical status of the backplane interface.

1.7 Configuration Examples

1.7.1 Configuring Backplane Interface Exception Alarms and Automatic Isolation

1. Requirements

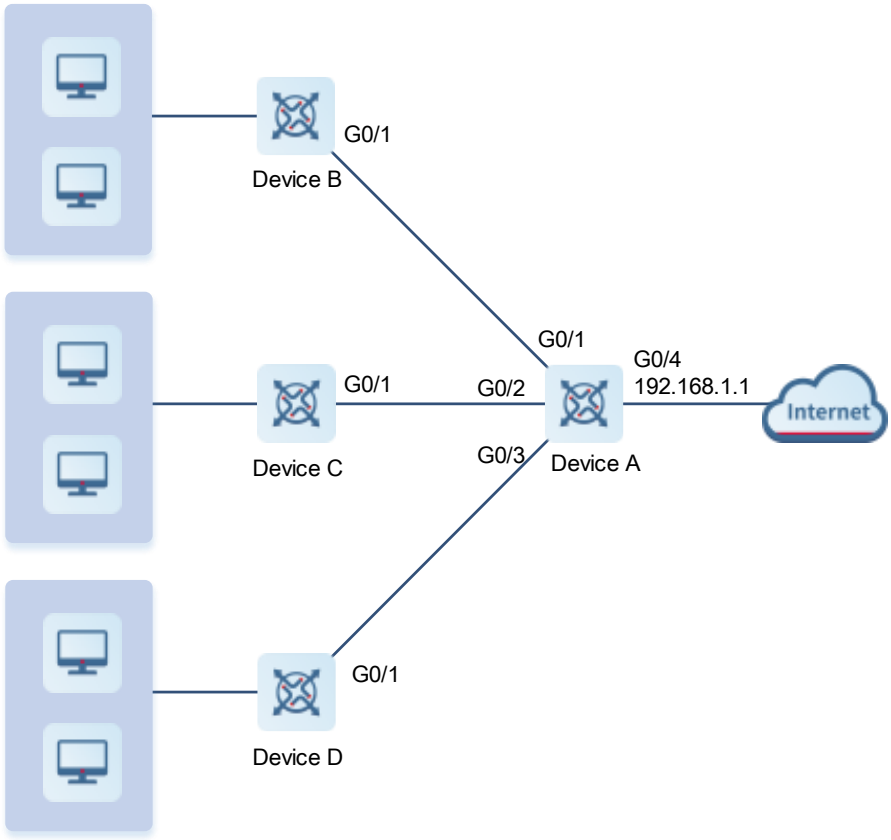
As shown in Figure 1-1, Device A is a core device. If its backplane interface is faulty, traffic of the entire network may be abnormal. To prevent the backplane interface fault on Device A from affecting intranet traffic forwarding, you need to configure the backplane interface exception alarm and automatic isolation on Device A.

- Set the polling period for backplane interface detection to **30** seconds.

- Set the maximum number of syslogs that are printed in each polling period to **10**.
- Enable the function of the backplane interface exception alarm.
- Automatically isolate the backplane interfaces that are detected abnormal in four detection periods.

2. Topology

Figure 1-1 Topology of Configuring Backplane Interface Exception Alarms and Automatic Isolation



3. Notes

- On Device A, configure the function of the backplane interface exception alarm.
- On device A, configure the automatic isolation function.

4. Procedure

Configure the function of the backplane interface exception alarm.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# fabric-interface polling-period 30
DeviceA(config)# fabric-interface warning limit 10
DeviceA(config)# fabric-interface warning crc-error on
DeviceA(config)# fabric-interface warning jitter on
DeviceA(config)# fabric-interface warning abnormal-down
```

Configure the automatic isolation function.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# fabric-interface isolate on
DeviceA(config)# fabric-interface isolate polling-cnt 4
```

5. Verification

Upon the preceding configurations, run the **show fabric-interface monitor plan** command to check the backplane interface exception alarm and automatic isolation for configuration.

```
DeviceA> enable
DeviceA# show fabric-interface monitor plan
          FABRIC-INTERFACE MONITOR-PLAN RELATIVE CONFIGURATIONS
------------------------------------------------------------------------------
Isolate-switch: ON
------------------------------------------------------------------------------
Polling-cnt: 4
Polling-period: 30
------------------------------------------------------------------------------
Warning-limit: 10
CRC-warning switch: ON
Jitter-warning switch: ON
Abnormal_down-warning switch: ON
```

6. Configuration Files

Device A configuration file

```
!
fabric-interface warning limit 10
fabric-interface polling-period 30
fabric-interface isolate on
fabric-interface isolate polling-cnt 4
!
```

Contents

1 Configuring Intelligent Monitoring 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Intelligent Temperature Monitoring 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, By default, the intelligent monitoring function is enabled after the device is powered on. Users can use this function without need of any configuration.

1.1.2 Intelligent Temperature Monitoring

The system continuously monitors temperature fluctuations during normal operation and promptly notifies users.

It defines two temperature thresholds: alarm threshold and hazard threshold. During intelligent monitoring, the system periodically polls all temperature points of the device.

When a temperature point reaches or exceeds the alarm threshold, a syslog is generated, and the alarm LED on the device's panel will turn yellow. When a temperature point reaches or exceeds the hazard threshold, a syslog is generated, and the alarm LED on the device's panel will turn red.

Warning

When the system detects that the device temperature exceeds the hazard threshold, it will only trigger a syslog and the red alarm LED on the device's panel, but will not shut down the device. Users should take immediate measures to cool the device, or power it down.

1.2 Monitoring

Run the **show** command to check the configuration.

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

Caution

During device operation, running the **clear** command may cause service interruption due to key information loss.

Table 1-1 Monitoring

Command	Purpose
show card voltage	Displays the voltage and voltage thresholds of devices.
show fan [[[*device-id*] *fan-id*] **detail** | **version**]	Displays fan information.

Command	Purpose
show temperature	Displays the device information such as current temperature and temperature thresholds.
show power	Displays power information about the device.
show temperature	Displays the device temperature and thresholds.

Contents

1 Configuring HDF 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 Basic Functions 2
1.4.1 Overview 2
1.4.2 Procedure 2
1.5 Configuring Single Real-time Diagnostics 3
1.5.1 Overview 3
1.5.2 Restrictions and Guidelines 3
1.5.3 Procedure 3
1.6 Configuring the HDF Alarm Function 3
1.6.1 Overview 3
1.6.2 Procedure 3
1.7 Configuring HDF Diagnostic Period 4
1.7.1 Overview 4
1.7.2 Procedure 4
1.8 Monitoring 4

1 Configuring HDF

1.1 Introduction

1.1.1 Overview

Hardware Diagnostics Function (HDF) is used to monitor status of hardware components on the device in real time. Network devices are made up of various semiconductor chips and components. After the devices run for a long period, components may experience functional failures due to factors such as the environment, external forces, and aging, which affects normal services. You can configure HDF to query the status of hardware components on the device in real time and automatically reports faults by using alarm notifications, Trap messages, and Syslog records.

1.1.2 Principles

Based on the idea of logical diagnostic nodes, HDF adopts unified logical diagnostic nodes for anomaly detection on hardware components, implementing various functions such as node management, detection mechanism, diagnostic analysis, self-healing actions, and log alarms.

The master nodes classified based on hardware component types include the CPU, storage, electromechanical module, logic module, Double Data Rate (DDR) Synchronous Dynamic Random Access Memory (SDRAM), interface optical module, and MAC switching chip. HDF supports splitting diagnostic items by using subnodes and provides management capabilities for diagnostic objects in three levels.

The functions provided by HDF are as follows:

- Enabling diagnostics/configuring the diagnostic period: You can enable HDF and configure the diagnostic period based on your service diagnostics requirements.
- Displaying the status of diagnostic objects: You can view the device hardware status, faulty component status, hardware status of specified slots, and diagnostic subnodes and items of slots.
- Single execution of all diagnostic nodes and items: HDF supports a single real-time execution of all enabled diagnostic nodes and items based on specific scenario requirements.

1.2 Restrictions and Guidelines

- The running environment of HDF includes a supervisor module, a line card, and a switch fabric module. When you configure HDF, ensure that the related components run properly.
- A diagnostic node dynamically registers for a card in the system. In this case, the information of some diagnostic nodes may fail to be queried instantly.

1.3 Configuration Task Summary

HDF configuration includes the following tasks:

(1) Configuring Basic Functions

(2) Configuring Single Real-time Diagnostics

(3) (Optional) Configuring the HDF Alarm Function

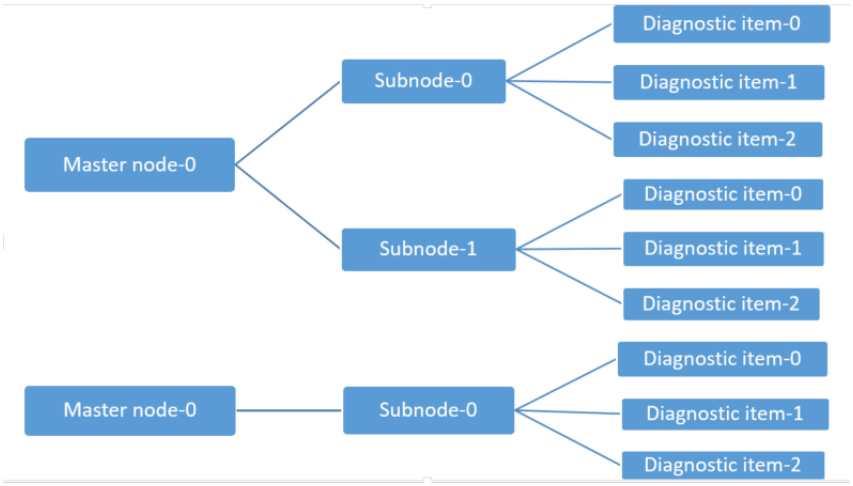
(4) (Optional) Configuring HDF Diagnostic Period

1.4 Configuring Basic Functions

1.4.1 Overview

You can perform management using HDF by configuring the diagnostic function on logical diagnostic nodes. Figure 1-1 shows the node management logic of HDF:

Figure 1-1 HDF Node Management



1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the HDF function. All the following configuration steps are optional. Perform the configuration steps as needed.

- Enable the HDF function for a card.

hdf enable { **all** | **slot** *slot-id* }

The HDF function is enabled for a single card by default.

- Enable the HDF function for the master node of a card.

hdf enable slot *slot-id* **main-node** *name*

The HDF function is enabled for the master node by default.

- Enable the HDF function for the subnode of a card.

hdf enable slot *slot-id* **main-node** *name* **child-node** *name*

The HDF function is enabled for the subnode by default.

- Enable the HDF function for specific diagnostic items of a card.

hdf enable slot *slot-id* [**main-node** *name* [**child-node** *name* [**item** *item-id*]]]

The HDF function is enabled for node diagnostic items by default.

1.5 Configuring Single Real-time Diagnostics

1.5.1 Overview

The diagnostics period of different components of a card vary. By default, a round-robin HDF diagnostics is performed for each item periodically. You can configure single real-time diagnostics in special scenarios. For example, you require that the status of a device and all diagnostic items are checked in real-time for troubleshooting the device during initial setup.

1.5.2 Restrictions and Guidelines

After you configure the single real-time diagnostics function, real-time diagnostics is performed for all enabled diagnostic nodes and diagnostic items of a card. You must enable diagnostic nodes and diagnostic items through commands before you perform real-time diagnostics.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure single real-time diagnostics for a card.

hdf once-run slot *slot-id*

After you configure this function, real-time diagnostics is performed for all enabled diagnostic nodes and diagnostic items of the card. You can run the **show hdf** command to display the diagnostic result.

1.6 Configuring the HDF Alarm Function

1.6.1 Overview

You can configure the HDF alarm function so that alarm logs are displayed when faults are detected by specific diagnostic items of a card.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the HDF alarm function for a card.

hdf alarm enable slot *slot-id* **main-node** *name* **child-node** *name* **item** *item-id*

The HDF alarm function is enabled for diagnostic items by default.

1.7 Configuring HDF Diagnostic Period

1.7.1 Overview

You can dynamically adjust the diagnostic period of diagnostic subnodes using Command Line Interface (CLI), which helps meet service diagnostics requirements.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the period of a node diagnostic item.

hdf set cycle slot *slot-id* **main-node** *name* **child-node** *name* **time** *cycle-number*

The default periods of node diagnostic items are the initialization values in service code.

1.8 Monitoring

Run the **show** command to check the information about the device hardware status.

Table 1-1 Monitoring

Command	Purpose
show hdf all	Displays the status of the hardware components of the device.
show hdf fault	Displays the status of the faulty hardware components of the device.
show hdf slot *slot-id* [**fault**]	Displays the status of the hardware components of a specific slot.
show hdf detail-info slot *slot-id* **main-node** *name* **child-node** *name* [**item** *item-id*]	Displays the status information about the diagnostic subnodes or diagnostic items of a slot.

Virtualization Configuration

1. Configuring VSU

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....14
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....15
1.4.4 Procedure....15
1.5 Configuring BFD-based DAD....16
1.5.1 Overview....16
1.5.2 Restrictions and Guidelines....16
1.5.3 Prerequisites....16
1.5.4 Procedure....16

1.6 Configuring Aggregate Interface-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 19
1.7.4 Procedure 19
1.8 Configuring VSU Attributes 19
1.8.1 Overview 19
1.8.2 Configuration Tasks 19
1.8.3 Configuring Basic VSU Attributes 20
1.8.4 Configuring Traffic Balancing 21
1.8.5 Switching to the Standalone Mode 21
1.8.6 Configuring Recovery Method for Recovery Mode 22
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 23
1.11 Configuration Examples 23
1.11.1 Setting Up a VSU 23

1.11.2 Configuring BFD-based DAD 26

1.11.3 Configuring Aggregate Interface-based DAD 29

1.12 Common Misconfigurations 33

1 Configuring VSU

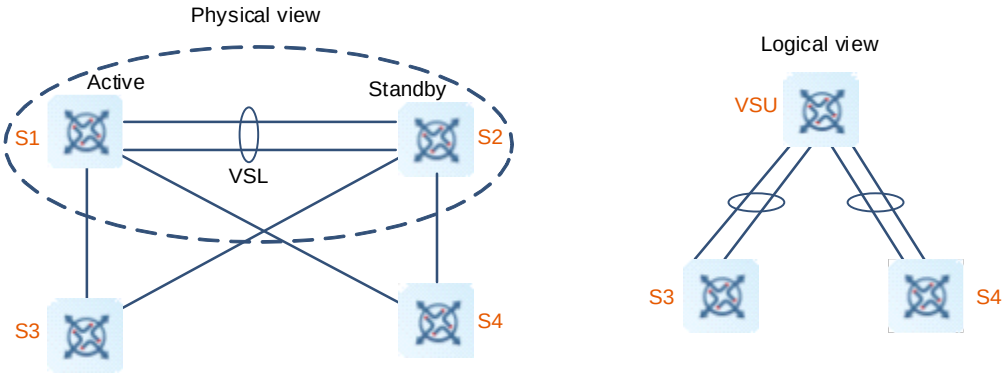
1.1 Introduction

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 device 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 device to form a VSU with the original device. Physically, the two devices seem to be one, and the original device backs up and sends the current configurations in batches to the new device. 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 device is equivalent to a port expansion card of the original device to increase port density.
- Higher forwarding capacity: If one device has a forwarding capacity of 14,400 Mpps, the entire VSU has a forwarding capacity of 28800 Mpps after one device is added.
- Larger bandwidth: If a 1000 M device 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

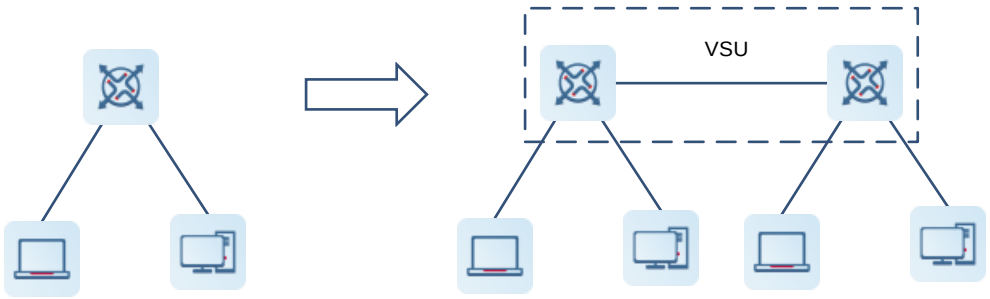


Figure 1-3 Forwarding Capacity Expansion over VSU

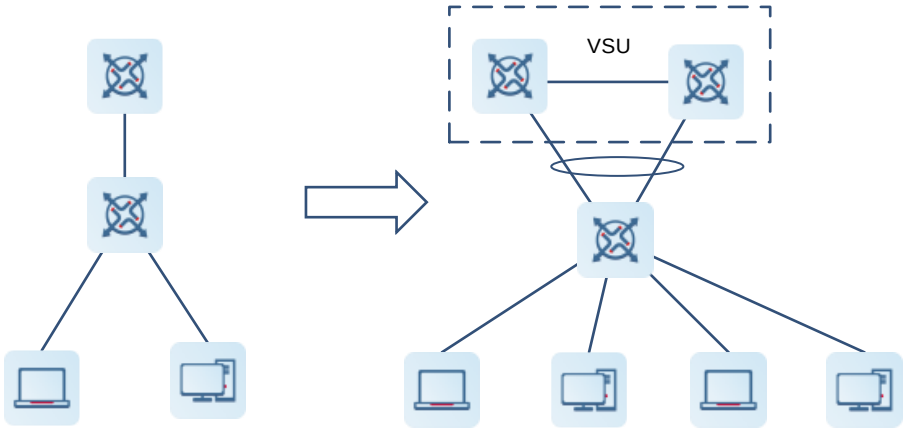
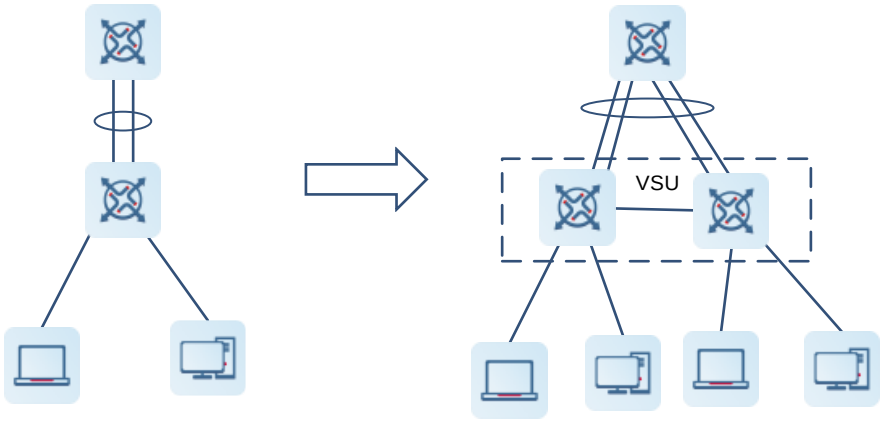


Figure 1-4 Bandwidth Expansion over VSU

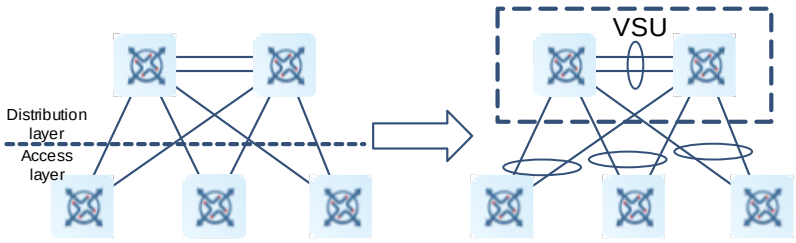


2. Simplified management

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 device is connected to two distribution devices 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 devices 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

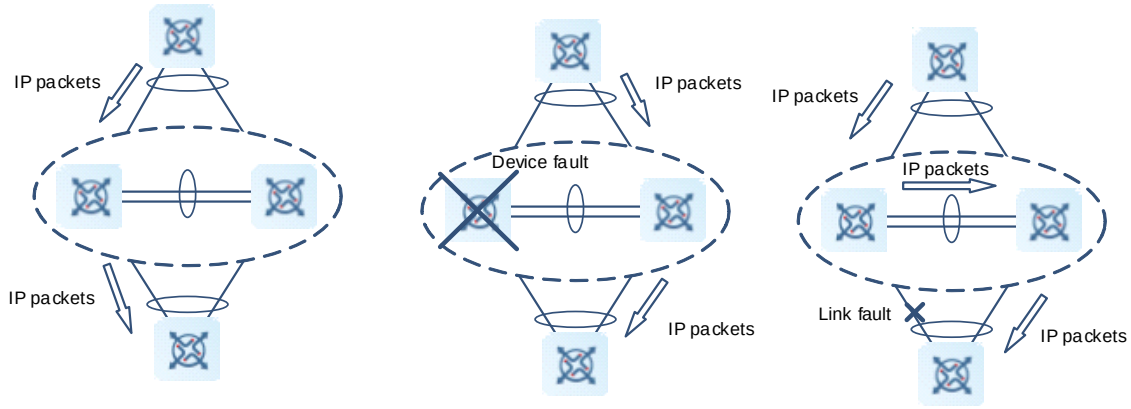
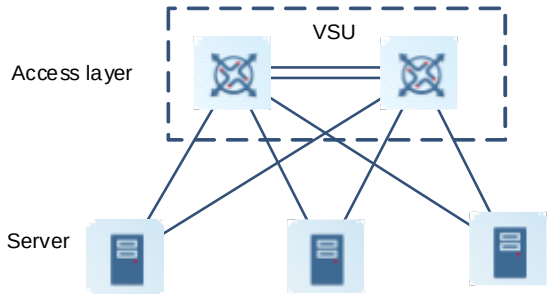


Figure 1-7 shows the typical application scenarios. Access servers with high availability requirements are connected with devices on the access layer by binding multiple network interface cards of a single server into an aggregation port. As the aggregation port allows access to only one access device, 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



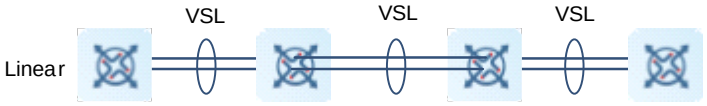
1.1.3 VSU Topology

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.

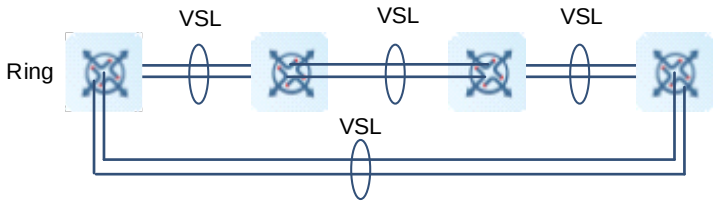
Figure 1-8 Linear Topology



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.

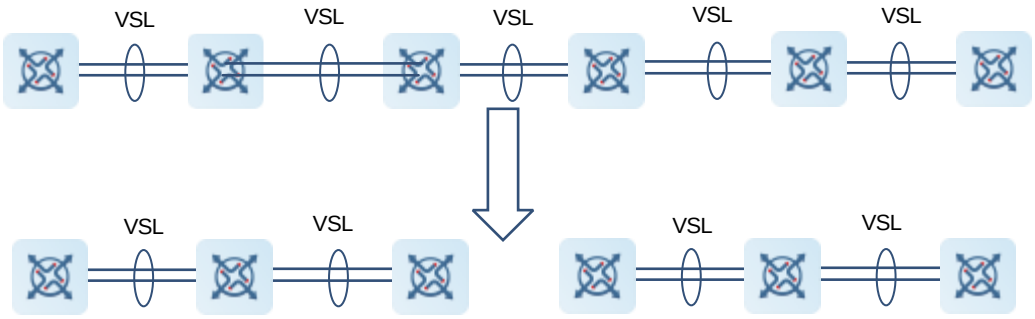
Note

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 link between the VSL and aggregate interface 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 section1.1.4 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 link between the VSL and aggregate interface. During topology combination, one of the VSUs automatically restarts in an attempt to join the other VSU, as shown in Figure 1-11.

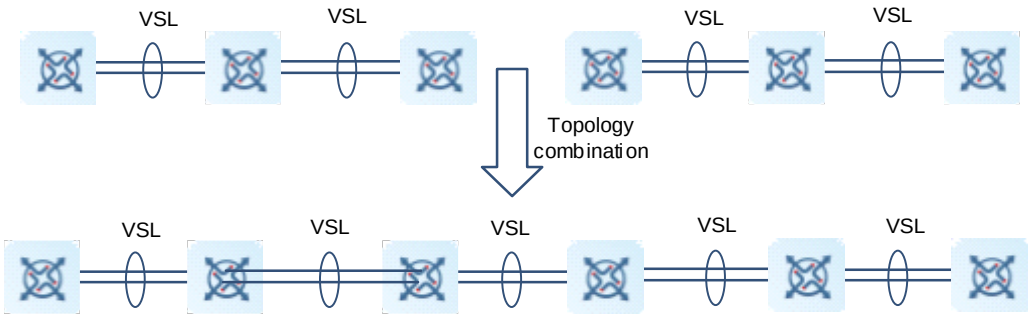
Topologies are combined based on the principle of minimizing the service impact caused by topology combination. The topology combination rules are as follows (topology combination starts from the first rule; if the optimal topology is not selected according to the first rule, the system goes on with 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



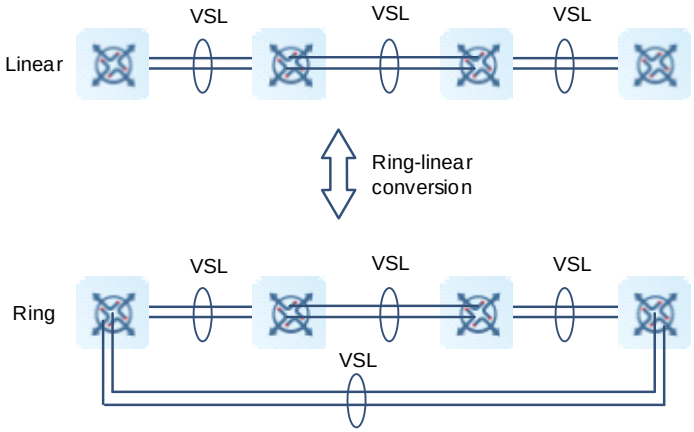
Note

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 link between the VSL and aggregate interface 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 links between the VSL and aggregate interface or nodes, troubleshoot the VSL fault in time for VSL recovery. After the link between the VSL and aggregate interface is recovered, the linear topology is converted back into a ring one.

Figure 1-12 Topology of Ring-Linear Conversion



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
- Aggregate interface-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 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.

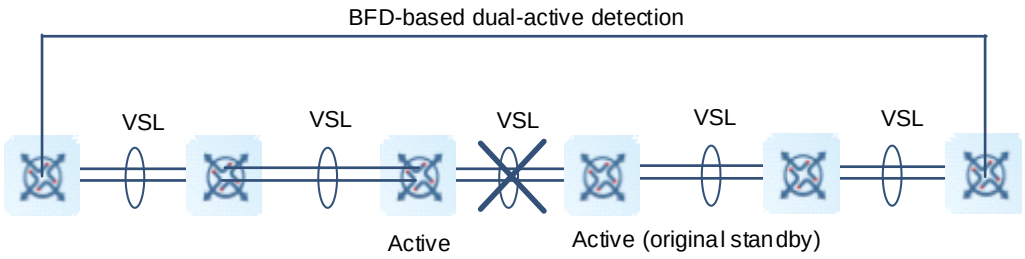
2. Keepalive Timer

To detect the link status of dual hosts, you can configure the Keepalive Timer. When it is detected that the link is deactivated and exceeds the keepalive interval, the dual host detection protocol will become invalid and dual host detection cannot be performed.

3. 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



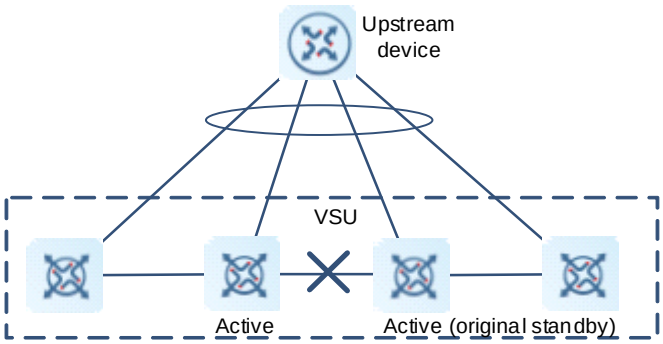
Caution

- 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.

4. Aggregate interface-based DAD

The VSU also supports the aggregate interface-based DAD mechanism. Figure 1-14 shows the connection topology. The VSU and the upstream device must support the aggregate interface-based DAD function. When the VSL port is disconnected, dual active devices coexist and send detection packets to each member port of the aggregate interface. The upstream device forwards the detection packets from one active device to the other. The aggregate interface 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 Aggregate Interface-based DAD



Specification

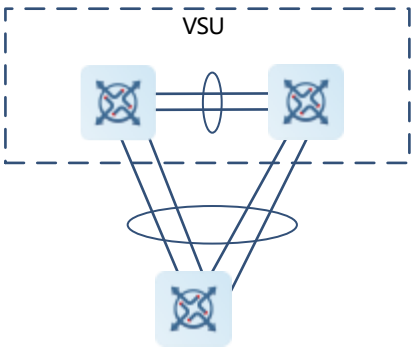
In the preceding topology, the upstream device must be a Ruijie device and can forward detection packets.

1.1.5 Traffic Forwarding

1. Cross-device Aggregation

An aggregate interface binds multiple physical links to form a logical link. The VSU supports an aggregate interface across member devices. As shown in Figure 1-15, two devices form a VSU and switch A is connected to the VSU as an aggregate interface. For switch A, the aggregate interface connections shown in the figure are equivalent to those of a common aggregate interface group.

Figure 1-15 Cross-device Aggregate Interface



A peripheral device is physically connected to each device in the VSU when a cross-device aggregate interface is configured. The advantages are as follows:

- Reserved bandwidth for the VSL: For cross-device aggregate interface traffic, the aggregate interface 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 aggregate interface faults and their impact:

Table 1-1 Cross-device Aggregate Interface Faults and Principle Description

Fault Scenario		Principle Description
Link fault	A single link of the aggregate interface is faulty.	The cross-device aggregate interface 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 aggregate interface are faulty.	The aggregate interface state changes to link down just as a common aggregate interface 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 aggregate interface redistributes traffic among the remaining normal links.
	The standby/candidate device is faulty.	The aggregate interface member ink connected to the member device is disconnected but other member links still work properly. The cross-device aggregate interface redistributes traffic among the remaining normal links.

2. Traffic balancing

In a VSU, traffic may have multiple egresses. The aggregate interface 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 aggregate interface 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. Line card naming

For chassis-type devices in VSU mode, device ID (switch ID) is added to the ID (name) of a line card. That is, the line card ID changes from 1-dimensional to 2-dimensional. For example, line card 1/1 represents the line card in slot 1 on a member device with the ID of 1.

3. 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, GigabitEthernet 1/1/1 indicates GE port 1 in slot 1 of a device with the ID of 1; GigabitEthernet 2/1/2 indicates GE port 2 in slot 1 of a device with the ID of 2.

4. 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.

5. 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.
- Most devices must use 10G ports as the VSL ports, depending on product specifications.
- 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.
- The configuration range of *switch-id* varies with product versions. If you update the device from a version with a large value range for *switch-id* to a version with a smaller value range for *switch-id*, the VSU configuration that involves the *switch-id* change may be lost. For example, originally, the value of *switch-id* can be set to the range of 1 to 6. After the device is updated, the value of *switch-id* can be set to the range of 1 to 4. The values 5 and 6 of *switch-id* become invalid. During device update, pay attention to the value range of *switch-id*. For more information, see restriction manual of the corresponding version.

1.3 Configuration Task Summary

The VSU configuration includes the following tasks:

(1) Setting Up a VSU

(2) Configuring BFD-based DAD

(3) Configuring Aggregate Interface-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 the 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 VSU 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 interface 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 type depends on the actual product version.

(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) port configured for DAD is switched to a Layer 2 (L2) 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 Layer-3 port to a Layer-2 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 Layer 2 Ethernet interface configuration mode.

interface *interface-type interface-number*

(4) Configure the BFD detection port as a Layer 3 Ethernet interface.

no switchport

A port is a Layer 2 Ethernet interface 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.

(10) (Optional) Configure the host detection link keepalive interval.

dual-active keepalive *interval*

By default, the dual-active link detection keepalive interval is 30 seconds.

1.6 Configuring Aggregate Interface-based DAD

1.6.1 Overview

The aggregate interface-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 Layer 3 port to a Layer 2 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 aggregate interface-based detection method.

dual-active detection aggregateport

The DAD function is disabled by default.

(5) Configure an aggregate interface-based detection port.

dual-active interface *interface-type interface-number* [**vlan** *vlan-id*]

No aggregate interface-based detection port is configured by default.

When the aggregated port is a trunk port and the native VLAN is beyond the VLAN range allowed by the aggregate interface-based detection port, configure a detection VLAN for the aggregate interface-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 link aggregation mode of the upstream and downstream devices, enable the function of forwarding aggregate interface-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.

(8) (Optional) Configure the host detection link keepalive interval.

dual-active keepalive *interval*

By default, the dual-active link detection keepalive interval is 30 seconds.

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 aggregate interface 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 aggregate interface after negotiation. Ports connected to the same device are in the same aggregate interface.
- During VSU running, configured VSL member links take effect immediately. VSL ports need to be configured on all devices.

- To prevent a loop from being instantaneously generated when a VSL member port exits the VSL aggregate interface, 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 aggregate interface, 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 interface 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 type of a VSL member port depends on the actual product version.

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 the 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, aggregate interface-based and ECMP-based Local Forward First (LFF) are enabled.
- In VSU mode, the cross-device aggregate interface-based LFF and ECMP-based LFF over Layer 3 ports are enabled by default. To set up a VSU with Layer 3 switches, you are advised to configure the aggregate interface-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 aggregate interface-based LFF.

no switch virtual aggregateport-lff enable

In VSU mode, the aggregated port-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 the 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 configuration.

Table 1-2 VSU Monitoring

Command	Purpose
show dad ap-port	Displays information about the DAD aggregate interface.
show dad bfd-port	Displays information about the BFD-enabled DAD interface.
show dad exclude-port	Displays the excluded interface for DAD.
show dad global-var	Displays variable information for DAD.
show dad relay-port	Displays information about the DAD forwarding interface.
show switch id	Displays the ID of the current device.
show switch virtual [**balance** | **config** | **role** | **topology**]	Views the topology, configurations, roles, and forwarding and balancing policies of the running VSU.
show switch virtual dual-active { **aggregateport** | **bfd** | **summary** }	Displays the information about the current DAD.
show switch virtual link [**port**]	Displays the information about the current VSL.
show vsl-dp app port *switch-id*	Displays VSL interface information.
show vsl-dp app sw *switch- id*	Displays the MAC address and number of VSL interfaces on a device.
show web-api virtual info [**device-id** *device-id*]	Displays the VSU configuration provided for the web.
show web-api virtual vsl-ports [**device-id** *device-id*]	Displays the configurable VSL interface information provided for the web.

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 a 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 VSU domain IDs (**domain-id**) are configured.
- The VSL ports are not up.

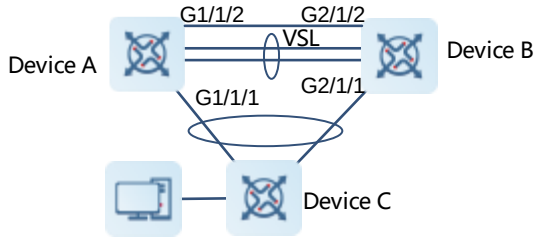
1.11.2 Configuring BFD-based DAD

1. Requirements

As shown in Figure 1-17, Device A and Device B form a VSU. 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).

Topology

Figure 1-17 Topology for BFD-based DAD



2. Notes

- Enable the BFD-based DAD.
- Designate a BFD detection port, which must be configured as a Layer 3 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.

3. 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
```

4. 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
```

5. 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
```

6. Common Errors

- The BFD-based detection port is not configured as a Layer 3 port.
- Either BFD-based or aggregate interface-based DAD is selected.

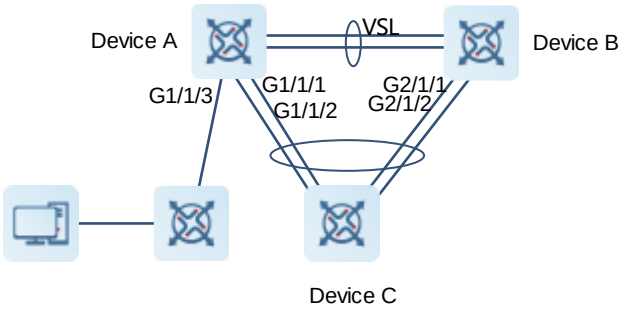
1.11.3 Configuring Aggregate Interface-based DAD

1. Requirements

As shown in **Figure 1-18**, Device A and Device B form a VSU, and Device C is connected to Device A and Device B separately over an aggregate interface. To prevent an IP address conflict in the LAN caused by two identical active devices in case of VSL disconnection, configure the aggregate interface-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 Aggregate Interface-based DAD



3. Notes

- Configure the ports connecting Device C to Device A and Device C to Device B as the same aggregate interface group.
- Enable the aggregate interface-based DAD.
- Configure the aggregate interface-based detection port.
- Configure the ports connecting Device C to Device A and Device B as the same aggregate interface group. Enable the function of forwarding aggregate interface-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 1/1/2, GigabitEthernet 2/1/1, and GigabitEthernet 2/1/2 to the aggregate interface 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)# exit
DeviceA(config)# interface range GigabitEthernet 2/1/1-2
DeviceA(config-if-range)# port-group 1
```

On Device A, enable the aggregate interface-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 aggregate interface 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
```

```
S57H3_206_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
S57H3_206_VSU-RECOVERY-2#sh switch virtual
Switch_id    Domain_id    Priority    Position    Status    Role
Description
------------------------------------------------------------------------------
------------
```

```
2(2)        100(100)     100(100)    LOCAL       Recovery   ACTIVE
S57H4-207
S57H3_206_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 aggregate interface detection port must be an aggregated port
- Either aggregate interface-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. Configuring Ethernet Interface
2. Configuring Aggregate Interface
3. Configuring PoE

Contents

1 Configuring Ethernet Interface 1
1.1 Introduction 1
1.1.1 Interface Classification 1
1.1.2 Interface Numbering Rules 2
1.2 Configuration Task Summary 3
1.3 Configuring Common Features of Ethernet Interfaces 4
1.3.1 Configuration Task Summary 4
1.3.2 Configuring Interfaces in a Range 4
1.3.3 Configuring Interface Description 5
1.3.4 Configuring Layer 2 or Layer 3 Interfaces 6
1.3.5 Configuring Interface Administrative Status 7
1.3.6 Configuring MTU of an Interface 8
1.3.7 Configuring Interface Bandwidth 9
1.3.8 Configuring Port Rates 10
1.3.9 Configuring the Flow Control Mode 10
1.3.10 Configuring the Duplex Mode of an Interface 12
1.3.11 Configuring the Auto Negotiation Mode 12
1.3.12 Configuring Protected Ports 13
1.3.13 Configuring EEE 14
1.3.14 Configuring Interface Traffic Statistics 15
1.3.15 Configuring SNMP Features for Interfaces 16
1.3.16 Configuring the Syslog Function for Interfaces 17

1.3.17 Configuring APD on Interfaces 18
1.4 Configuring Optical Transceiver Features 18
1.4.1 Configuration Task Summary 18
1.4.2 Configuring Information Collection Intervals of Optical Transceivers 19
1.4.3 Configuring Alarm Detection for Optical Transceivers 19
1.4.4 Configuring Optical Transceiver Antifake Detection 20
1.5 Configuring the MAC Address of an Interface 20
1.5.1 Overview 20
1.5.2 Restrictions and Guidelines 21
1.5.3 Procedure 21
1.6 Configuring Port Reliability Attributes 21
1.6.1 Configuration Task Summary 21
1.6.2 Configuring the Carrier-Delay for an Interface 21
1.6.3 Configuring Port Flapping Protection 22
1.6.4 Configuring Interface Diagnostics 23
1.6.5 Configuring Port Errdisable Recovery 23
1.6.6 Testing Connected Cable Status 24
1.6.7 Configuring CRC Error Frame Alarm Detection for an Interface 25
1.6.8 Configuring 10G Optical Ports to Support 2.5 Gbps 26
1.7 Monitoring 26
1.8 Configuration Examples 28
1.8.1 Configuring Interface Attributes 28
1.8.2 Configuring Interconnection Interfaces 32

1 Configuring Ethernet Interface

1.1 Introduction

Interfaces are important in implementing data switching on network devices. The company's 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, 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 Interface Classification

- Layer 2 interface

  A Layer 2 interface is a single physical port on a device and implements only the Layer 2 switching function.

- Layer 3 interface

  A physical port on a Layer 3 device can be configured as a Layer 3 interface, which functions as the gateway interface for Layer 3 switching. A Layer 3 interface does not have the Layer 2 switching function or associate with VLANs. Therefore, it can be used only as an access interface.

- Aggregate interface

  An aggregate interface is a logical link that is formed by binding multiple physical ports together. After the physical ports are bound as an aggregate interface, the bandwidths of the physical ports are added up, which expands the link bandwidth. The interfaces that are bound as an aggregate interface must be of the same type, to be specific, all of them are Layer 3 interfaces or Layer 2 interfaces. Packets that pass the aggregate interface can be distributed to the members of the aggregate interface. If a member link of the aggregate interface becomes invalid, the aggregate interface automatically transfers the traffic on this faulty link to other valid member links, improving reliability of connections.

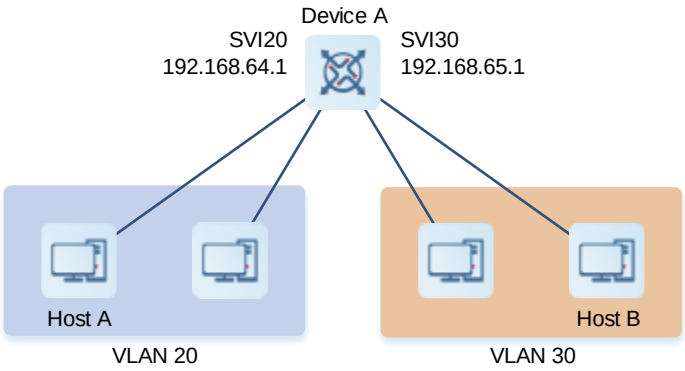
- Switch virtual interface (SVI)

  An SVI acts as a management port of al 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 a specific virtual local area network (VLAN) to implement routing across VLANs among Layer 3 devices.

  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 Layer 3 devices. If Host A in VLAN 20 wants to communicate with Host B in VLAN 30, SVI 20 of VLAN 20 and SVI 30 of VLAN 30 must be used.

Figure 1-1 Schematic Diagram of SVI



- Loopback interface

  The loopback interface is a local Layer 3 logical interface simulated by software. The loopback interface is a virtual Ethernet interface that is always in the up state. 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 a device ID of the Open Shortest Path First (OSPF) routing protocol, an IP address for access to a telnet server, or a source IP address for access by a telnet client.

1.1.2 Interface Numbering Rules

Table 1-1 shows the numbering rules of physical ports on the devices supporting or not supporting daughter cards in the standalone mode or virtual switch unit (VSU) mode.

Table 1-1 The Numbering Rules of Physical Ports

Daughter Cards	Stand-alone mode	VSU mode
Not Support	A physical port number consists of the slot number and port number on the slot. For example, if the slot number of the port is 2, and the port number on the slot is 3, the port ID is 2/3.	A physical port number consists of the device number, slot number and port number on the slot. For example, if the device number is 1, slot number is 2, and port number on the slot is 3, the port ID is 1/2/3.
Support	A physical port number consists of the slot number, card number and port number on the slot. For example, if the slot number of the port is 2, the card number is 1 and the port number on the slot is 3, the port ID is 2/1/3.	A physical port number consists of the device number, slot number, card number and port number on the slot. For example, if the device number is 1, the slot number of the port is 2, the card number is 1 and the port number on the slot is 3, the port ID is 1/2/1/3.

The numbering rules of the preceding devices, slots, daughter cards, and ports on slots or cards are as follows:

- 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.
- Daughter card ID: On a line card supporting daughter cards, the daughter card ID is 0. The daughter card ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Dynamic daughter card slots are numbered from 1 sequentially from left to right, and from top to bottom.
- The port ID on a slot or a daughter card ranges from 0 to the number of ports on the slot, and is numbered sequentially from left to right.

In addition to physical ports, a device also has logical interfaces. The numbering rules of logical interfaces are as follows:

- The ID of a link aggregation ranges from 1 to the number of link aggregations supported by the device.
- The ID of an SVI is the VLAN ID corresponding to this SVI.

1.2 Configuration Task Summary

The following tasks are optional. Select them as need.

- Configuring Common Features of Ethernet Interfaces

  The following tasks are optional. Select them as need.

  - Configuring Interfaces in a Range
  - Configuring Interface Description
  - Configuring Layer 2 or Layer 3 Interfaces
  - Configuring Interface Administrative Status
  - Configuring MTU of an Interface
  - Configuring Interface Bandwidth
  - Configuring Port Rates
  - Configuring the Flow Control Mode
  - Configuring the Duplex Mode of an Interface
  - Configuring the Auto Negotiation Mode
  - Configuring Protected Ports
  - Configuring Interface Traffic Statistics
  - Configuring SNMP Features for Interfaces
  - Configuring the Syslog Function for Interfaces
  - Configuring APD on InterfacesConfiguring the Syslog Function for Interfaces
- Configuring Optical Transceiver Features

  The following tasks are optional. Select them as need.

  - Configuring Information Collection Intervals of Optical Transceivers
  - Configuring Alarm Detection for Optical Transceivers
  - Configuring Optical Transceiver Antifake Detection
- Configuring the MAC Address of an Interface

- Configuring Port Reliability Attributes

  The following tasks are optional. Select them as need.

  - Configuring the Carrier-Delay for an Interface
  - Configuring Port Flapping Protection
  - Configuring Interface Diagnostics
  - Configuring Port Errdisable Recovery
  - Configuring CRC Error Frame Alarm Detection for an Interface

1.3 Configuring Common Features of Ethernet Interfaces

1.3.1 Configuration Task Summary

The following tasks are optional. Select them as required.

- Configuring Interfaces in a Range
- Configuring Interface Description
- Configuring Layer 2 or Layer 3 Interfaces
- Configuring Interface Administrative Status
- Configuring MTU of an Interface
- Configuring Interface Bandwidth
- Configuring Port Rates
- Configuring the Flow Control Mode
- Configuring the Duplex Mode of an Interface
- Configuring the Auto Negotiation Mode
- Configuring Protected Ports
- Configuring Interface Traffic Statistics
- Configuring SNMP Features for Interfaces
- Configuring the Syslog Function for Interfaces

1.3.2 Configuring Interfaces in a Range

1. Overview

For physical ports or logical interfaces created, enter the batch configuration mode of the interfaces within a specified range. For logical interfaces have not been created, the system will create specified logical interfaces in a batch and enter the batch configuration mode of the interfaces within a specified range. When you enter the batch configuration mode to configure multiple interfaces at a time, the attributes configured apply to all interfaces in the selected range.

Run the **interface range** command 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. 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. Run the **no define interface-range macro-name** to remove the configuration.

2. Restrictions and Guidelines

- For logical interfaces, you can run the **no interface range** command to bacth delete the interfaces in a specified range. But this command cannot batch delete physical ports.
- Run the **default interface range** command to restore the default configuration of the interfaces within a specified range in the interface configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure a macro name for the interfaces to be configured in a batch.

define interface-range *macro-name interface-type interface-range-string*

The default macro name is not configured for the interfaces to be configured in a batch.

(4) Enter the batch configuration mode.

interface range { *interface-type interface-range-string* | **macro** *macro-name* }

The default interface range is not configured.

1.3.3 Configuring Interface Description

1. Overview

Configure a name for an interface to identify the interface and help you remember the functions of the interface.

For example, if you want to assign GigabitEthernet 0/1 for exclusive use by user A, describe the interface as "Port for User A."

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

- Enter the Loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the description for the interface.

description *interface-name*

The default interface name is not configured.

1.3.4 Configuring Layer 2 or Layer 3 Interfaces

1. Overview

A physical port and an aggregate interface on a Layer 3 device can be configured as Layer 3 interfaces and function as the gateway interfaces for Layer 3 switching. A Layer 3 interface cannot be used for Layer 2 switching. You can run the **no switchport** command to change a Layer 2 interface to a Layer 3 interface and assign an IP address to this interface to set up a route. You can run the **switchport** command to change a Layer 3 interface to a Layer 2 interface.

2. Restrictions and Guidelines

- Running the **no switchport** command will delete all Layer 2 features of the interface.
- A Layer 2 link aggregation with member ports cannot be configured as a Layer 3 link aggregation, and vice versa.
- When a port is a member port of a Layer 2 link aggregation or an unauthenticated dot1x port, you cannot change the port type using the **switchport** command or the **no switchport** command.

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 Layer 2 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 2 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*

(4) Configure an interface as a Layer 2 or Layer 3 Interface. Perform at least one of the following configuration tasks:

- Configure an interface as a Layer 2 interface.
  switchport
- Configure an interface as a Layer 3 interface.
  no switchport

  All the interfaces are Layer 2 interfaces by default.

  All ports are switch ports by default.

1.3.5 Configuring Interface Administrative Status

1. Overview

Enter the interface mode to disable or enable an interface. 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. 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.

2. Restrictions and Guidelines

The errdisable ports can be recovered using the **shutdown** or **no shutdown** command. To prevent unwanted link flapping caused by frequently running the **shutdown** or **no shutdown** command, there should be a certain time interval, which must be greater than the carrier delay of the interface, before you run the **shutdown** or **no shutdown** command again on an 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*

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*
- Enter the Layer 2 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI interface configuration mode.
  interface vlan *interface-number*
- Enter the Loopback interface configuration mode.
  interface loopback *interface-number*

(4) Disable the interface.

shutdown

An interface is enabled by default.

1.3.6 Configuring MTU of an Interface

1. Overview

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.

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. If you want a device to receive and handle Jumbo frames, configure the MTU greater than the length of a jumbo frame for the device.

2. Restrictions and Guidelines

- Configuring the system MTU will update the MTU effective values of all the Ethernet interfaces (including the link aggregations) of the system. However, if the interface is configured with an MTU, the MTU configured for the interface will take effect.
- You can set an MTU for an interface to control the maximum length of frames that can be received or forwarded by the interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an MTU. Configure at least one of the following tasks.

a Configure the system MTU.

system mtu *mtu-value*

No default system MTU is configured.

b Enter the interface configuration mode.

interface *interface-type interface-number*

- Enter the Layer 2 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 2 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI interface configuration mode.
  interface vlan *interface-number*

c Configure the MTU of an interface.

mtu *mtu-value*

The MTU of an interface is 1500 by default. The value range of this parameter depends on the actual product version.

The MTU values configured for virtual interfaces (including SVI interfaces,) and the MTU values configured by the **ip mtu** command must be smaller than or equal to the MTU values configured for the actual physical interfaces. If the MTU values are not properly configured, the packets whose lengths exceed the MTU values of physical interfaces will be discarded.

1.3.7 Configuring Interface Bandwidth

1. Overview

This 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.

2. Restrictions and Guidelines

The **bandwidth** command is a routing parameter, and does not affect the bandwidth of a physical link.

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*

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

- Enter the Loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the bandwidth for an interface.

bandwidth *bandwidth-value*

No default interface bandwidth is configured.

1.3.8 Configuring Port Rates

1. Overview

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.

If the interface rate is set to the **auto** mode, the interface rate can be automatically adjusted based on the type of the inserted module. Currently supported modules include small form-factor pluggable (SFP) and enhanced SFP (SFP+) modules. 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. This function takes effect only when the interface rate is set to the **auto** mode.

2. Restrictions and Guidelines

- If an interface is a member port of a link aggregation, the rate of this interface depends on the rate of the link aggregation. After an interface exits a link aggregation, it will use its own rate.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

(4) Configure the port rate:

speed { **10** | **100** | **1000** | **10G** | **auto** }

The interface rate is set to auto by default.

1.3.9 Configuring the Flow Control Mode

1. Overview

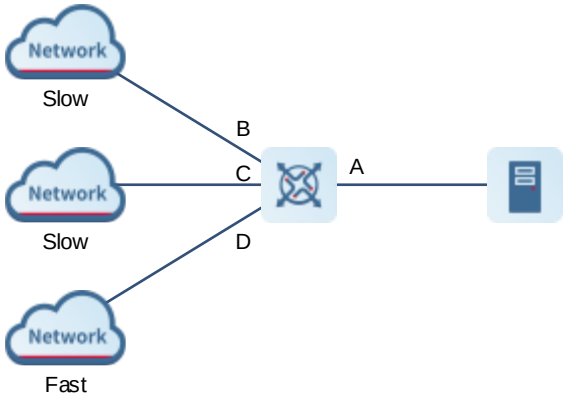
There are two flow control modes of an interface:

- 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.

- Asymmetric flow control mode: When an interface works in the asymmetric flow control mode, the interface processes the received flow control frames but does not forward flow control frames.
- The flow control mode of a link aggregation takes effect on all member links.

As shown in Figure 1-2, Port A of the device is an uplink port, and Ports B, C and D are downlink ports. Port B and Port C are connected to different slow networks. Port A is enabled with the functions of sending and receiving flow control frames. As Port B and Port C are connected to different slow networks, if a large amount of data is sent on Port B, Port B and Port C will be congested. Then 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, 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



2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(4) Configure the flow control mode of an interface.

flowcontrol { **auto** | **off** | **on** }

The flow control mode is disabled by default.

1.3.10 Configuring the Duplex Mode of an Interface

1. Overview

The duplex mode of an interface can be configured based on the duplex mode of a peer interface. You can specify one of the following work modes for the interface:

- 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.

2. Restrictions and Guidelines

When you configure the duplex mode of a link aggregation, the configuration takes effect on all of its member ports.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

(4) Configure the duplex mode.

duplex { **auto** | **full** | **half** }

An interface is in auto-negotiation mode by default.

1.3.11 Configuring the Auto Negotiation Mode

1. Overview

- 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.
- 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.

2. Restrictions and Guidelines

- When you configure the auto-negotiation mode for an aggregate interface, the configuration takes effect on all of its member interfaces.
- For a 100 M 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**.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(4) Configure the auto negotiation mode for the interface.

negotiation mode { **off** | **on** }

The auto negotiation mode of an interface is disabled by default.

1.3.12 Configuring Protected Ports

1. Overview

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.

2. Restrictions and Guidelines

Two protected ports cannot communicate with each other. But when they 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 link aggregation can be configured as a protected port. When a link aggregation is configured as a protected port, all of its member ports are configured as protected ports. By default, the Layer 3 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Block Layer 3 routing between protected ports.

protected-ports route-deny

Layer 3 routing is not blocked between protected ports by default.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(5) Configure a protected port.

switchport protected

No interface is configured as a protected port by default.

1.3.13 Configuring EEE

1. Overview

Energy Efficient Ethernet (EEE) is an Ethernet solution that saves 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 low power idle (LPI) mode to save 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, a port automatically enters LPI mode if the port is always up without sending or receiving any packet in a period of time. The port switches to 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.

2. Restrictions and Guidelines

- 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.

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 Layer 2 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(4) Enable EEE on the interface.

eee enable

EEE is disabled on an interface by default.

1.3.14 Configuring Interface Traffic Statistics

1. Overview

By default, virtual interfaces such as SVIs does 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 the **show interface** *interface-type interface-number* command to view the packet statistics of the specified interface and IP packet statistics.

The default statistics collection interval of an Ethernet interface is five seconds, that is, interface statistics are updated every five seconds. To meet high requirements for real-time statistics, prolong the collection interval.

The statistics of default sending and receiving rates of a device does not include interframe gaps. The sending and receiving rates of physical layer packets refers to the packet sending and receiving rates including the number of packet bytes and interframe gaps. If you wants to check the sending and receiving rates of physical layer packets, enable the device to calculate interframe gaps when it calculates the packet sending and receiving rates. Then the statistics will display the sending and receiving rates of physical layer packets. After the function is enabled, the interframe gap size is fixed at 20 bytes, which consists of 12-byte frame gaps and 8-byte preambles. There is deviation because the device calculates 12-byte frame gaps while the command statistics exclude frame gaps.

2. Restrictions and Guidelines

- Enabling the interface traffic statistics collection function and IP traffic statistics collection function consumes system resources. Enable the functions as required.
- A shorter collection interval consumes more system performance. Therefore, adjust the collection interval as required. You are advised to set the collection interval to more than 10 seconds if there are over 500 physical interfaces.
- After you run the **flow-statistics include-interframe enable** command, the device will clear the statistics of the packet sending and receiving rates of the interface and calculate the rates again.
- You can run the **show interfaces transceiver** command to view the optical module information that is collected periodically and the **show interface** [*interface-type interface-number*] **transceiver** command to view the real-time optical module information on the specified interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the collection interval for Ethernet interface statistics collection.

ethernet-port counter sample-period [*interval*]

The default collection interval of Ethernet interface statistics collection is five seconds.

(4) Configure that the interface rate statistics include interframe gaps.

flow-statistics include-interframe enable

The interface rate statistics does not include interframe gaps by default.

(5) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

- Enter the Loopback interface configuration mode.

  interface loopback *interface-number*

(6) Enable the traffic statistics collection function on the interface.

statistics { **ip enable** }

The IP traffic statistics collection function is disabled on all interfaces by default.

(7) (Optional) Configure the interval of load calculation for the interface.

load-interval *interval*

The interval of load calculation for an interface is 10 seconds by default.

1.3.15 Configuring SNMP Features for Interfaces

1. Overview

The Simple Network Management Protocol (SNMP) is used for network monitoring and management. Because many manufactures support SNMP, it becomes a network management standard and is widely used in manufactures' interconnection systems. Through SNMP, a network administrator can check information, configure networks, locate faults and plan capacity for network nodes for network nodes. Our devices support following SNMP features.

- 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. Enable the interface index persistence feature to retain the interface index after you

restart the device.

- Enhanced name display for interfaces

  After enhanced name display for interfaces is enabled in a standard MIB node, the value of an interface name 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 of an interface name in a standard MIB node and the interface name do not contain spaces. In addition, the ifName node displays the short name of the interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable interface index persistence for the interface.

snmp-server if-index persist

The interface index persistence feature is disabled on an interface by default.

(4) Configure enhanced name display for interfaces.

snmp-server if-name enhance

The function is disabled by default.

After you run this command, save the configuration and restart the device to make the configuration take effect. Then the interface names obtained by SNMP will not contain spaces.

1.3.16 Configuring the Syslog Function for Interfaces

1. Overview

Use the syslog function to determine whether to display information about interface changes or exceptions.

Enable or disable the syslog function as required. By default, this function is enabled. When an exception occurs on an interface, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the syslog printing function on the interface.

logging [**error-frame** | **insert-remove** | **link-dither** | **link-updown** | **res-lack-frame**]

The syslog printing function is enabled on an interface.

(4) Enter the Ethernet interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*

(5) Configure interface information printing.

logging [**link-updown** | **link-state realtime**]

By default, the prompt information about the interface status change is printed, while the real-time information about the interface link status change is not printed.

1.3.17 Configuring APD on Interfaces

1. Overview

Auto Power Down (APD) is a method to save energy. When an Ethernet interface is not connected, the interface enters Power-Down mode to save energy. When the APD function is not enabled, the interface that is not connected to a network cable will continuously provide power, which will cause waste of electric energy. In APD mode, the interface automatically listens to the signal of the link. If no signal is detected on the link (for example, no network cable is plugged in), the interface automatically enters Power-Down mode. If a signal is detected on the link (the network cable is plugged in), power supply is resumed.

2. Restrictions and Guidelines

- Running the **show auto-power-down** command can display the APD information on an interface.

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 Layer 2 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

(4) Configure the APD function on the interface.
auto-power-down enable

By default, the APD function is enabled on an interface.

1.4 Configuring Optical Transceiver Features

1.4.1 Configuration Task Summary

The following tasks are optional. Select them as required.

- Configuring Interfaces in a Range

1.4.2 Configuring Information Collection Intervals of Optical Transceivers

1. Overview

If there is a high requirement for information collection timeliness, you can shorten the information collection period of the optical transceiver, so that the maintenance personnel can obtain information changes of the optical transceiver in time.

2. Restrictions and Guidelines

- A shorter collection interval consumes more system performance. Therefore, adjust the collection interval as required.
- Run the **show interfaces transceiver** command to query periodically collected optical transceiver information. Run the **show interface** [*interface-type interface-number*] **transceiver** command to display the real-time optical transceiver information of a specified interface. Run the **show interfaces transceiver register-dump** command to display optical transceiver register information.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the information collection interval of optical transceivers on Ethernet interfaces.

ethernet-port fiber-info sample-period [*interval*]

The default information collection interval of optical transceivers on Ethernet interfaces is five minutes.

1.4.3 Configuring Alarm Detection for Optical Transceivers

1. Overview

After this function is configured, you can view the optical transceiver alarm information of an interface by using the management information base (MIB). When events such as insertion or removal of an optical transceiver, optical transceiver exceptions, and optical transceiver exception clearing are detected, related TRAP messages are sent. The exceptions include overhigh/overlow transmit power of the optical transceiver, overhigh/overlow receive power of the optical transceiver, inter-integrated circuit (IIC) fault of the optical transceiver, 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 transceiver 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 transceiver insertion or removal, but sends a TRAP message in the next period for optical transceiver exceptions and optical transceiver exception clearing. 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.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the alarm detection function for optical transceivers.

fiber alarm-detect enable

The alarm detection function is enabled for optical transceivers by default.

(4) (Optional) Configure the alarm detection period for optical transceivers.

fiber alarm-detect period *minutes*

The default alarm detection period of optical transceiver exceptions is 10 minutes.

(5) (Optional) Configure the periodic repeated notification mode of optical transceiver alarms.

fiber alarm-detect repeat-mode { **on** | **off** }

The repeated notification mode of optical transceiver alarms is enabled by default.

1.4.4 Configuring Optical Transceiver Antifake Detection

1. Overview

Configure the optical transceiver antifake detection function to check whether the optical transceiver in use is supplied by our company.

If the optical transceiver is not supplied by our company, the data communication may be affected. If the optical transceiver antifake detection function is enabled, the device can automatically identify an optical transceiver that is not supplied by our company and generate an alarm when such a module is inserted to our company's device.

This function is disabled by default. You can enable this function through configuration.

Each optical transceiver supplied by our company has a unique antifake code. The device can read this antifake code to determine whether the module is supplied by our company. If not, the device will generate syslogs and send trap messages.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure optical transceiver antifake detection.

fiber antifake { **ignore** | **enable** }

The optical transceiver antifake detection function is disabled by default.

1.5 Configuring the MAC Address of an Interface

1.5.1 Overview

Each Layer 3 Ethernet interface has a globally unique MAC address. Our company's device supports modifying the MAC addresses of Ethernet interfaces. However, MAC addresses in the same LAN must be unique.

1.5.2 Restrictions and Guidelines

Configuration of MAC addresses may affect internal communication in a LAN. You are advised not to change the MAC address of the Layer 3 Ethernet interface in normal cases.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

(4) Configure the MAC address of an interface.

mac-address *mac-address*

The system uses factory settings by default.

1.6 Configuring Port Reliability Attributes

1.6.1 Configuration Task Summary

The following tasks are optional. Select them as required.

- Configuring the Carrier-Delay for an Interface
- Configuring Port Flapping Protection
- Configuring Interface Diagnostics
- Configuring Port Errdisable Recovery

1.6.2 Configuring the Carrier-Delay for an Interface

1. Overview

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.

2. Restrictions and Guidelines

- If the DCD carrier interruption time is long, set a smaller carrier delay so that the routing protocol learns

about link state changes more quickly, thereby accelerating topology and route convergence.

- If the DCD carrier interruption time is shorter than the network topology or route summarization time, set a larger carrier delay (relative to carrier interruption time) to avoid frequent route flapping.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

- Enter the Loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the carrier-delay for an interface.

carrier-delay { [**milliseconds**] *delay-interval* | **up** [**milliseconds**] *up-interval* **down** [**milliseconds**] *down-interval* }

By default, the delay after which the DCD signal changes from **down** to **up** is 2s, and the delay after which the DCD signal changes from **up** to **down** is 0s.

1.6.3 Configuring Port Flapping Protection

1. Overview

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.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the port flapping protection function.

physical-port dither protect

The port flapping protection function is enabled by default.

(4) (Optional) Configure the port flapping protection parameters.

physical-port dither period *period-time* **threshold** *threshold-number* **period-times** *continuous-period*

By default, the port flapping detection interval is 2s, the threshold for triggering periodic flapping counting within an interval is 6 times, and the number of continuous periods during which flapping suppression is triggered is 10,

1.6.4 Configuring Interface Diagnostics

1. Overview

When an interface is faulty, you can implement interface diagnostics using a command. The diagnostics result and fault information are displayed during interface diagnostics. View the diagnostics information to quickly find the fault cause. Run the **show interface** [*interface-type interface-number*] **troubleshooting** command to display the recent diagnostic information of an interface in privileged EXEC mode.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enabling interface diagnostics.

troubleshooting interface *interface-type interface-number*

Interface diagnostics is not enabled on an interface by default.

1.6.5 Configuring Port Errdisable Recovery

1. Overview

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 will occur if the number of addresses learned on this port exceeds the maximum number of security addresses. Protocols, such as the Spanning Tree Protocol (STP), 802.1x, Rapid Ethernet Uplink Protection Protocol (REUP) and port flapping protection support the similar functions.

2. Restrictions and Guidelines

- 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, 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. In addition, you can run the **shutdown** or **no shutdown** command to recover all the ports in the errdisable state and enable If the problem causing port errdisable is not fixed, the port will enter the errdisable state again.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Configure port errdisable recovery in the privileged EXEC mode.

errdisable recovery cause link-state

By default, the port errdisable recovery function is disabled.

(3) Enter the global configuration mode.

configure terminal

(4) Configure port errdisable recovery in the global configuration mode.

errdisable recovery [**cause link-state** | **cause uplink-detect | interval** *interval*]

By default, the port errdisable recovery function is disabled.

For some specified errdisable recovery functions, **cause link-state** can be configured in privileged EXEC mode or global configuration mode. Choose one mode to configure it. If **cause link-state** has been configured in privileged EXEC mode, it does not need to be configured in global configuration mode.

(5) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 2 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*

(6) Configure the port errdisable recovery interval.

errdisable recovery interval *interval*

By default, the port errdisable recovery interval is not configured.

1.6.6 Testing Connected Cable Status

1. Overview

An administrator uses cable detection commands to detect the operating status of a cable. Cable detection helps to identify the operating status of a cable when the cable is short-circuited, disconnected, or in another abnormal state.

2. Restrictions and Guidelines

- Only an electrical port supports cable detection. An optical port or a link aggregation does not support cable

detection.

- Performing cable detection on a normally connected interface causes a temporary disconnection.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(4) Test the operating status of a connected cable.

line-detect

1.6.7 Configuring CRC Error Frame Alarm Detection for an Interface

When an interface receives a CRC error frame, it indicates faults such as service packet loss occur on the link. An alarm will be triggered in the form of printing Syslog and sending the alarm TRAP on an Ethernet interface with CRC error frame alarm detection enabled if CRC error frame statistics exceeding the alarm threshold is detected for several consecutive sampling periods. Restrictions and Guidelines

In order to avoid alarm flapping, keep a gap between *alarm-threshold* and *resume-threshold*.

1. Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Enter the Ethernet interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(4) Enable CRC error alarm detection.
port-detect crc-frame enable

CRC error alarm detection is enabled by default.

(5) (Optional) Configure the alarm threshold and recovery threshold for the number of CRC error packets.
port-detect crc-frame alarm-threshold *alarm-value* **resume-threshold** *resume-value*

By default, the alarm threshold for the number of CRC error packets on the interface is 500, and the recovery threshold is 50.

(6) (Optional) Configure the number of periods for CRC error alarm detection.

port-detect crc-frame period-times *period-number*

The number of periods for CRC error alarm detection on an interface is 5 by default.

1.6.8 Configuring 10G Optical Ports to Support 2.5 Gbps

Due to chip constraints of products, the 10G optical port does not support the rates of 1 Gbps, 2.5 Gbps, and 10 Gbps at the same time. You can run the **port speed-cap** command to configure a 10G optical port to support the rates of 1 Gbps and 2.5 Gbps.

4. Restrictions and Guidelines

This command takes effect after the device is restarted.

When a 10G optical port is configured to support 2.5 Gbps, the system returns a response indicating a successful rate downgrade to 2.5 Gbps, and a response indicating a failed rate downgrade to 1 Gbps. By default, a 10G optical port is successfully downgraded to 1 Gbps, but fails to be downgraded to 2.5 Gbps.

The 10 Gbps rate configuration for a 10G optical port is not affected.

5. Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Configure the 10G optical port to support 2.5 Gbps.
port speed-cap 2500

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.

Caution

Services may be interrupted due to loss of vital information if you run the **clear** command during device operation.

Table 1-2 Ethernet Interface Monitoring

Command	Purpose
show auto-power-down	**Displays the APD status on an interface.**
show interfaces [*interface-type interface-number*]	Displays all the statuses and configuration information of a specified interface.
show interfaces [*interface-type interface-number*] **status**	Displays the interface status.
show interfaces [*interface-type interface-number*] **status detail**	Displays detailed interface status information.

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 interface.
show interfaces [*interface-type interface-number*] **switchport**	Displays the status information of Layer 2 interfaces.
show interfaces [*interface-type interface-number*] [**description**] [**up | down**]	Displays the configuration and status of an interface.
show interfaces [*interface-type interface-number*] **counters** [**up | down**]	Displays the statistics of a specified port.
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 errors** [**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.
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.
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 ethernet brief [**up** | **down**]	Displays the information about Ethernet interfaces in Up or Down state.
show interfaces *interface-type interface-number* **ethernet brief**	Displays the brief information about an Ethernet interface.
show interfaces [*interface-type interface-number*] **fault-info**	Displays the fault information about an interface.
show interfaces [*interface-type interface-number*] **troubleshooting**	Displays the diagnosis information about an interface.

show interfaces usage [**up | down**] **show interfaces** *interface-type interface-number* **usage**	Displays the bandwidth usage of an interface.
show interfaces [*interface-type interface-number*] **mtu forwarding**	Displays the information of the forwarding plane MTU.
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.
show interfaces [*interface-type interface-number*] **transceiver diagnosis**	Displays the current measurement values of optical module diagnosis parameters of a specified interface.
show interfaces [*interface-type interface-number*] **transceiver register-dump**	Displays information about the optical transceiver register on a specified interface.
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.
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 cause and fault occurrence time of an interface.

1.8 Configuration Examples

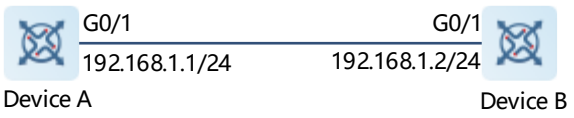
1.8.1 Configuring Interface Attributes

1. Requirements

Interconnect two devices, and configure the basic attributes of the device interfaces.

2. Topology

Figure 1-3 Topology of Configuring Interface Attribute



3. Notes

- Connect two devices through Layer 2 interfaces.

- 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 respectively as follows:

- Run the **shutdown** command on the interface GigabitEthernet 0/1, and check whether GigabitEthernet 0/1 and SVI 1 are in **Down** state.
- Run the **shutdown** command on the interface GigabitEthernet 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 GigabitEthernet 0/1 is the same as that before the restart.

Device A:

```
DeviceA# 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
```

```
  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
  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
  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
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

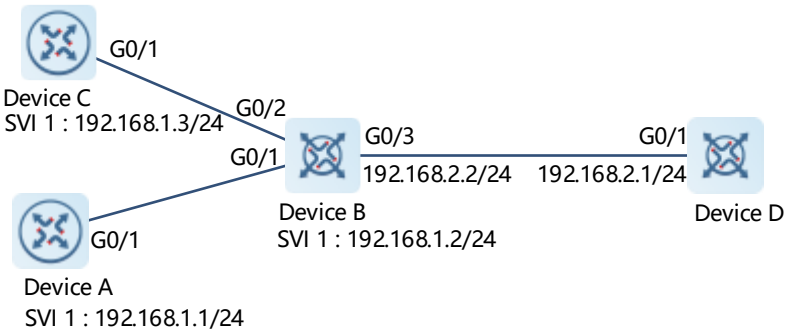
1.8.2 Configuring Interconnection Interfaces

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 Layer 2 interface in access mode, and set the default VLAN ID to 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 Layer 2 interfaces in trunk mode, and set the native VLAN ID to 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a Layer 3 interface, and assign an IP address in another network segment to this interface.
- On Device C, configure GigabitEthernet 0/1 as Layer 2 interface in access mode, and set the VLAN ID to 1. Configure SVI 1, and assign an IP address to SVI 1.
- On Device D, configure GigabitEthernet 0/1 as a Layer 3 interface, assign an IP address to this interface, 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 respectively 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 status of GigabitEthernet 0/1 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
  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 the status of GigabitEthernet 0/1 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
  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 the status of GigabitEthernet 0/1 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
  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 the status of GigabitEthernet 0/1 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
  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 Interface 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Load Balancing 4
1.1.3 Member Port BFD Detection 5
1.1.4 Protocols and Standards 5
1.2 Configuration Task Summary 5
1.3 Configuring Static Aggregate Interfaces 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 6
1.3.3 Procedure 7
1.4 Configuring LACP Interfaces 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 8
1.4.3 Procedure 8
1.5 Enabling LinkTrap 10
1.5.1 Overview 10
1.5.2 Procedure 10
1.6 Configuring a Load Balancing Mode 10
1.6.1 Overview 10
1.6.2 Procedure 10
1.7 Enabling BFD for Member Ports 11

1.7.1 Overview 11
1.7.2 Restrictions and Guidelines 11
1.7.3 Procedure 11
1.8 Configuring the Minimum Number of Member Ports 11
1.8.1 Overview 11
1.8.2 Restrictions and Guidelines 12
1.8.3 Procedure 12
1.9 Enabling the LACP Independent Port Function 13
1.9.1 Overview 13
1.9.2 Restrictions and Guidelines 13
1.9.3 Procedure 13
1.10 Monitoring 13
1.11 Configuration Examples 15
1.11.1 Configuring Static Aggregate Interfaces 15
1.11.2 Configuring LACP Interfaces 16
1.11.3 Enabling LinkTrap 18
1.11.4 Configuring a Load Balancing Mode 20
1.11.5 Enabling BFD for Member Ports 22
1.11.6 Configuring the Minimum Number of Member Ports (When the Number of Member Ports Is Less Than the Minimum Number) 25
1.11.7 Configuring the Minimum Number of Member Ports (When the Number of Member Ports Is Not Less Than the Minimum Number) 27
1.11.8 Enabling the LACP Independent Port Function 29

1 Configuring Aggregate Interface

1.1 Introduction

An aggregate interface 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 aggregate interface supports load balancing, that is, distributes load evenly among member links. Besides, an aggregate interface realizes link backup. When a member link of the aggregate interface 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 link aggregation. One is the static aggregate interface mode, and the other is dynamic aggregation through Link Aggregation Control Protocol (LACP).

1. Static Aggregate Interface

The static aggregate interface mode means manually configuring physical ports and adding them to a link aggregation group. An aggregate interface in static aggregate interface mode is called a static aggregate interface, and its member ports are called member ports of a static aggregate interface. The static aggregate interface configuration is simple. You only need to run a command to add the specified physical port to the aggregate interface. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

2. Dynamic Aggregate Interface (LACP)

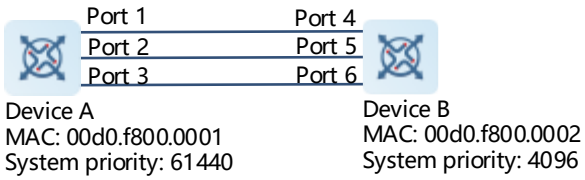
LACP is a protocol about dynamic link aggregation. It exchanges information with the connected device through link aggregation control protocol data units (LACPDU). An aggregate interface in LACP mode is called a dynamic aggregate interface, and its member ports are called member ports of a dynamic aggregate interface.

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 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. Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

Member ports in active mode initiate LACP negotiation. Member ports in passive mode only respond to received LACPDUs. 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. Member Port State

Static 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 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 aggregate interface cannot be added to or removed from a static aggregate interface or an LACP aggregate interface.

5. Capacity Mode

The maximum number of member ports is fixed, which is equal to the maximum number of aggregate interfaces multiplied by the maximum number of member ports supported by a single aggregate interface. If you want to increase the maximum number of aggregate interfaces, the maximum number of member ports supported by a single aggregate interface must be reduced, and vice versa. This concerns the aggregate interface capacity mode concept. Some devices support the configuration of the aggregate interface capacity mode. For example, if the system supports 16,384 member ports, you can select 1024 x 16, 512 x 32, and other aggregate interface capacity modes (Maximum number of aggregate interfaces multiplied by the maximum number of member ports supported by a single aggregate interface).

6. LACP System ID

By default, all the LACP interfaces on a device belong to the same LACP aggregation group.

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 interfaces of multiple (a maximum of four) independent devices need to negotiate with the LACP interface of a specific device (for example, LACP interfaces of two independent ASWs need to negotiate with the LACP interface of the NC). You can set the system IDs of the LACP interfaces 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 interfaces of multiple independent devices need to negotiate with the LACP interface of a specific device. It must be configured together with the system ID.

8. LACP Port ID

Each port has an independent LACP interface priority, which is a configurable value. The port ID consists of the LACP interface 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. Minimum Number of Member Ports

An aggregate interface can be configured with a minimum number of member ports. When a member port exits the link 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 aggregate interface 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 aggregate interface is **Up** again.

11. 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 aggregate interface 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 member port again.

1.1.2 Load Balancing

Aggregated ports 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 link aggregation 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 + L4 destination port number
- Source IP address + destination IP address + L4 source port number + L4 destination port number
- Panel port for incoming packets
- Aggregation member port polling

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.

1.1.3 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 aggregate interface, 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 aggregate interface configuration includes the following tasks:

(1) Configuring Static

(2) (Optional) Configuring LACP Interfaces

(3) (Optional) Enabling LinkTrap

(4) (Optional) Configuring a Load Balancing Mode

(5) (Optional) Enabling BFD for Member Ports

(6) (Optional) Configuring the Minimum Number of Member Ports

(7) (Optional) Enabling the LACP Independent Port Function

(8) (Optional) Configuring the Active/Standby Member Interface Function for the Link Aggregate Port

1.3 Configuring Static Aggregate Interfaces

1.3.1 Overview

- Configure multiple physical ports as 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 aggregate interface 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 aggregate interface.
- Before adding an interface to a static AP, run the **shutdown** command in the interface configuration mode to avoid flapping. After the interface and its peer interface are added to the corresponding static APs, run the **no** form of the shutdown command.
- To prevent a transient loop when a member port exits, you need to set the member port to **shutdown** state before it exits the aggregate interface.
- The ports of different medium types or port modes cannot be added to the same aggregate interface.
- L2 ports can be added to only a L2 aggregate interface, and L3 ports can be added to only a L3 aggregate interface. The L2/L3 attributes of an aggregate interface that contains member ports cannot be modified.
- After a port is added to an aggregate interface, the attributes of the port are replaced by those of the aggregate interface.
- After a port is removed from an aggregate interface, the attributes of the port before the adding to the aggregate interface are restored.
- There is continuous traffic at the aggregate interface. If a member port changes from **Link Up** to **Link Down**, an error may occur in traffic statistics of the aggregate interface.
- You can run the **port-group** command to add a physical port to a static aggregate interface in the interface configuration mode of the specified Ethernet port. If the aggregate interface does not exist, it will be created automatically.
- You can run the **port-group mode** command to add a physical port to an LACP aggregate interface in the interface configuration mode of the specified physical port. If the aggregate interface does not exist, it will be created automatically.
- The aggregate interface feature must be configured on the devices at both ends of a link and the aggregate interface mode must be the same (static aggregate interface or LACP aggregate interface).

- After a member port exits the aggregate interface, the default configurations of the member port may be restored. The original configurations of aggregate interface 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 aggregate interface.
- After a member port exits an aggregate interface, 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 member port of L3 aggregate interface exits the aggregate interface, the port may be switched to a L2 port.
- The aggregate interface created on a L3 device that does not support L2 features is a L3 aggregate interface; otherwise the aggregate interface is a L2 aggregate interface.

Warning

- After a port is added to an aggregate interface, the attributes of the port are consistent with those of the aggregate interface. Therefore, it is generally not allowed to perform configuration on the member ports or apply configurations to a specific member port. However, some commands or functions (such as the **shutdown** and **no shutdown** commands) can be configured on the member ports. When using the member ports, you need to check whether the function that you want to configure can take effect on a specific 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 aggregate interface.

interface aggregateport *ap-number*

Perform this configuration on an aggregate interface-enabled device. When an Ethernet port needs the aggregation function, create the corresponding Ethernet aggregate interface

No aggregate interface is configured by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure member ports of a static aggregate interface.

port-group *ap-number*

Perform this configuration on aggregate interface-enabled devices. To use the static aggregation function, configure the corresponding member ports of a static aggregate interface.

By default, the Ethernet physical port does not belong to any static aggregate interface or LACP aggregate interface.

(6) (Optional) Convert L2 aggregate interfaces to L3 aggregate interfaces.

no switchport

The aggregate interface is a L2 port by default.

1.4 Configuring LACP Interfaces

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 aggregate interface 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 aggregate interface, the default configurations of the port may be restored. The original configurations of LACP 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 aggregate interface.
- To prevent a transient loop when a member port exits, you need to set the member port to **shutdown** state before it exits the aggregate interface.
- Changing the LACP system priority may cause LACP member ports to be disaggregated and aggregated again.
- Changing the priority of an LACP member port may cause the other member ports to be disaggregated and aggregated again.
- There is continuous traffic at the aggregate interface. If a member port changes from **Link Up** to **Link Down**, an error may occur in traffic statistics of the aggregate interface.
- The LACP 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) (Optional) Configure the LACP system priority.

lacp 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 aggregate interface.

The LACP system priority of a port is 32768 by default.

(4) Configure the timeout interval of the LACP system in short timeout mode.

lacp short-timeout period *interval*

The timeout interval of the LACP system is 3 seconds in short timeout mode by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) Configure LACP member ports.

port-group *key-number* **mode** { **active** | **passive** }

By default, the Ethernet physical port does not belong to any LACP aggregate interface.

(7) Configure the priority of an LACP 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 member port is 32768 by default.

(8) Configure the timeout mode of LACP 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 member port is long timeout by default.

(9) Return to the global configuration mode.

exit

(10) Enter the aggregate interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface aggregateport *interface-number*

(11) (Optional) Configure the LACP system ID.

lacp system-id *system-id*

Configure the LACP system ID when LACP interfaces of multiple (a maximum of four) independent devices need to negotiate with the LACP interface of a specific device.

The LACP system ID is the system ID (MAC address) of the device by default.

(12) (Optional) Configure the LACP device ID.

lacp device *number*

Configure the LACP device ID when LACP interfaces of multiple (a maximum of four) independent devices need to negotiate with the LACP interface of a specific device.

The device ID is 0 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 aggregate interface configuration mode.

interface Aggregateport *ap-interface-number*

(4) (Optional) Configure the LinkTrap function of an aggregate interface.

snmp trap link-status

The LinkTrap notification function of an aggregate interface is enabled by default.

(5) (Optional) Configure the LinkTrap function of member ports.

aggregateport member linktrap

The LinkTrap notification function of 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 aggregate interface performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

1.6.2 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 aggregate interface.

aggregateport load-balance { **dst-ip** | **dst-mac** | **ip** | **src-dst-ip** | **src-dst-ip-l4port** | **src-dst-ip-src-dst-l4port** | **src-dst-mac** | **src-ip** | **src-mac** | **src-port** }

By default, for a device on which an aggregate interface is created as a L2 aggregate interface by default, load is distributed according to the source MAC addresses and destination MAC addresses of the incoming packets.

1.7 Enabling BFD for Member Ports

1.7.1 Overview

- Enable BFD for all the member ports of a specified aggregate interface.
- After BFD is enabled for an aggregate interface, 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.

1.7.2 Restrictions and Guidelines

- After BFD is enabled for an aggregate interface, 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 member port is not supported. You must enable or disable BFD for the entire aggregate interface 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.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*

(4) (Optional) Configure BFD for 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 a member port is disabled by default.

1.8 Configuring the Minimum Number of Member Ports

1.8.1 Overview

- After the minimum number of 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 aggregation group is greater than or equal to the sum of bandwidth provided by member ports of aggregate interfaces.
- After an action for the minimum number of member ports is configured, for example, shutting down the aggregate interface, the action is triggered when the number of member ports in **Up** state is less than the minimum number of the member ports.

1.8.2 Restrictions and Guidelines

- If the number of member ports for an LACP interface is less than the minimum number of member ports of the aggregate interface configured, all member ports are in the unbinding state, and the peer end is also automatically unbound.
- After the minimum number of member ports of a static aggregate interface is configured, if the number of member ports of a static aggregate interface in **Up** state is less than the minimum number, the member ports of a static aggregate interface in **Up** state cannot forward data and the corresponding aggregate interface 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 member ports is configured, the action is triggered only when the number of 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 member ports decreases from 3 or more to less than 3.

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.

- Enter the Layer 2 aggregate interface configuration mode.

interface aggregateport *ap-number*

- Enter the Layer 3 aggregate interface configuration mode.

interface aggregateport *ap-number*

(4) (Optional) Configure the minimum number of member ports.

aggregateport member minimum { *port-number* | **action shutdown** }

Perform this configuration to specify the minimum number of the member ports of a link aggregation.

The minimum number of member ports of an aggregate interface is 1 by default.

(5) (Optional) Configure the action triggered when the number of 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 member ports in **Up** state is less than the minimum number of member ports.

By default, no action is configured for the minimum number of member ports in an aggregate interface.

1.9 Enabling the LACP Independent Port Function

1.9.1 Overview

- After the LACP independent port function is enabled, an LACP member port automatically changes to a common physical port if the LACP member port does not receive LACP packets within the set timeout period. The LACP member port state is changed to individual and the LACP member port can forward packets properly.
- After the LACP 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.

1.9.2 Restrictions and Guidelines

- After the LACP independent port function is enabled, an LACP member port does not immediately change to a common physical port. Instead, the LACP 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 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.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (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.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) (Optional) Enable the LACP independent port function.

lacp individual-port enable

Perform this operation so that an LACP member port can forward packets normally when the LACP member port cannot perform LACP negotiation.

The LACP independent port function is disabled by default.

1.10 Monitoring

Run the **show** command to check the configuration.

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

Caution

- Running the **clear** command during operation of the device may lose vital information and interrupt services.

Table 1-2 Aggregate Interface Monitoring

Command	Purpose
show aggregateport capacity	Displays the capacity mode and usage of an aggregate interface.
show aggregateport load-balance	Displays the load balancing information of an aggregate interface.
show aggregateport [*ap-number*] **summary**	Displays the summary of an aggregate interface.
show lacp capacity	Displays the LACP capability of the device.
show lacp counters [*key-number*]	Displays the statistics of LACP packets on LACP member ports. You can view the information of a specified LACP interface by specifying **key-number**.
show lacp counters [*key-number*]	Displays LACPDU statistics on member interfaces of the aggregate interface.
show lacp information gr	Displays LACP data synchronization information.
show lacp information ha	Displays LACP hot standby information.
show lacp information pkt-agent [**pkt_count** | **port** { *interface-index* | *interface-type interface-number* }]	Displays LACP proxy information.
show lacp information pkt_count	Displays packet statistics of an LACP process.
show lacp information port [*interface-index* | *interface-type interface-number* | **all**]	Displays LACP interface information.
show lacp information port-version	Displays the version number of the interface.
show lacp summary [*key-number*]	Displays the state of an LACP interface. You can view the information of a specified LACP interface by specifying **key-number**.
clear lacp counters [*key-number* | *interface-type interface-number*]	Clears the statistics of LACP packets on an LACP member port.

1.11 Configuration Examples

1.11.1 Configuring Static Aggregate Interfaces

1. Requirements

Create aggregate interface interconnection for two devices on the IPv4 network, and configure static aggregate interfaces.

2. Topology

Figure 1-2 Topology for Configuring Static Aggregate Interfaces

3. Notes

- Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Device A to static aggregate interface 3.
- Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Device B to static aggregate interface 3.

4. Procedure

Create aggregate interface 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 aggregate interface 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 aggregate interface 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
!
```

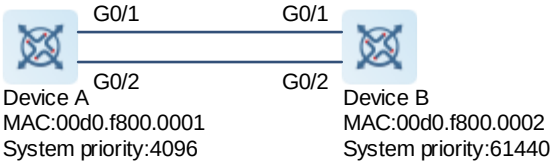
1.11.2 Configuring LACP Interfaces

1. Requirements

Create aggregate interface interconnection for two devices on the IPv4 network, and configure dynamic aggregate interfaces.

2. Topology

Figure 1-3 Topology for Configuring LACP Ports



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 interface 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 interface 3.

4. Procedure

Configure LACP Ports 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 Ports 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 interface 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
!
```

1.11.3 Enabling LinkTrap

1. Requirements

On the IPv4 network, create aggregate interface interconnection for two devices, configure static aggregate interfaces, and enable LinkTrap.

2. Topology

Figure 1-9 Topology for Enabling LinkTrap

3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static aggregate interface 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static aggregate interface 3.
- On Device A, disable LinkTrap for aggregate interface 3 and enable LinkTrap for its member ports.
- On Device B, disable LinkTrap for aggregate interface 3 and enable LinkTrap for its 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 aggregate interface 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
!
```

1.11.4 Configuring a Load Balancing Mode

1. Requirements

On the IPv4 network, create aggregate interface interconnection for two devices, configure static aggregate interfaces, and enable load balancing.

2. Topology

Figure 1-10 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 aggregate interface 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static aggregate interface 3.
- On Device A, configure source MAC address-based load balancing for aggregate interface 3 in global configuration mode.
- On Device B, configure destination MAC address-based load balancing for aggregate interface 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
!
```

1.11.5 Enabling BFD for Member Ports

1. Requirements

Create aggregate interface interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-11 Topology for Enabling BFD for 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 interface 3.
- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B and add the ports to LACP interface 3.
- Configure IP address 1.0.0.1 for aggregate interface 3 on Device A and enable IPv4 BFD.
- Configure IP address 1.0.0.2 for aggregate interface 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 running-config** to check whether the configuration is correct. to check whether the configuration is correct.

Run **show interface aggregateport** to view the BFD state of each 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 aggregate interface without BFD parameters, BFD does not take effect.
- After BFD is enabled for an aggregate interface, the BFD neighbor must be a directly connected aggregate interface enabled with BFD.

1.11.6 Configuring the Minimum Number of Member Ports (When the Number of Member Ports Is Less Than the Minimum Number)

1. Requirements

On the IPv4 network, create aggregate interface interconnection for two devices, and configure the number of member ports less than the minimum number of member ports.

2. Topology

Figure 1-12 Topology for Configuring the Minimum Number of Member Ports (When the Number of Member Ports Is Less Than the Minimum Number)

3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP interface 3.
- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet0/2 ports on Device B and add the ports to LACP interface 3.
- On Device A, set the minimum number of the member ports of aggregate interface 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 running-config** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each 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
!
```

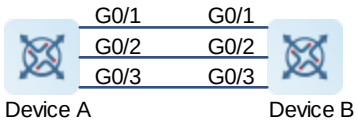
1.11.7 Configuring the Minimum Number of Member Ports (When the Number of Member Ports Is Not Less Than the Minimum Number)

1. Requirements

On the IPv4 network, create aggregate interface interconnection for two devices, and configure the number of member ports not less than the minimum number of member ports.

2. Topology

Figure 1-13 Topology for Configuring the Minimum Number of Member Ports (When the Number of Member Ports Is Not Less Than the Minimum Number)



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 interface 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 interface 3.
- On Device A, set the minimum number of member ports of aggregate interface 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 running-config** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each 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
!
```

1.11.8 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 interface, for example, aggregate interface 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 1-14 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 interface 3.

- Enable the LACP independent port function for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device.
- Allocate aggregate interface 3 on the access device to VLAN 10.

4. Procedure

Create an aggregate interface 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 running-config** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each 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
!
```

Contents

1 Configuring PoE 1
1.1 Introduction 1
1.1.1 Basic Concepts 1
1.1.2 Power Supply Management for the PoE System 1
1.1.3 Power Supply Management for PoE Ports 2
1.1.4 Auxiliary PoE Power Supply Functions 3
1.1.5 LLDP Classification 3
1.1.6 Upgrading the MCU Firmware 4
1.1.7 Power Supply Management for PoE Line Cards 4
1.1.8 Protocols and Standards 4
1.2 Configuration Task Summary 4
1.3 Configuring Power Supply of the PoE System 4
1.3.1 Overview 4
1.3.2 Restrictions and Guidelines 5
1.3.3 Procedure 5
1.4 Configuring Power Supply on PoE Ports 5
1.4.1 Overview 5
1.4.2 Restrictions and Guidelines 6
1.4.3 Procedure 6
1.5 Configuring Auxiliary PoE Power Supply Functions 7
1.5.1 Overview 7
1.5.2 Restrictions and Guidelines 7

1.5.3 Procedure....7
1.6 Configuring LLDP Classification....8
1.6.1 Overview....8
1.6.2 Restrictions and Guidelines....8
1.6.3 Procedure....8
1.7 Monitoring....8
1.8 Configuration Examples....9
1.8.1 Configuring Power Supply of the PoE System....9
1.8.2 Configuring Power Supply on PoE Ports....10
1.8.3 Configuring Auxiliary PoE Power Supply Functions....11
1.8.4 Enabling the LLDP Classification....11

1 Configuring PoE

1.1 Introduction

Power over Ethernet (PoE) is a technology that can be used to transmit electricity and data to devices through twisted pairs over Ethernet. This technology enables various devices such as voice over Internet Protocol (VoIP) phones, Wi-Fi access points (APs), network cameras, hubs and computers to directly obtain electricity from twisted pairs.

1.1.1 Basic Concepts

1. PoE

PoE power supplies power the entire PoE system and are classified into external and internal power supplies. The box-type PoE devices of Ruijie are usually equipped with internal power supplies. Some products also support external power supplies. An external power supply is called a redundant power supply (RPS).

2. PSE

Power sourcing equipment (PSE) searches for and detects powered devices (PDs) on PoE ports, classifies the PDs into different classes, and supplies power to the PDs. After detecting that a PD is removed, the PSE stops supplying power to the PD.

3. PD

PDs are devices powered by PSE and are classified into standard PDs and non-standard PDs. Standard PDs are PDs that comply with the IEEE 802.3af and 802.3at standards. Common non-standard PDs include non-standard PDs with featured resistance, Cisco pre-standard PDs, PDs supporting only signal cable power supplies, and PDs supporting only idle cable power supplies. Ruijie devices use signal cable power supplies and do not support PDs supporting only idle cable power supplies.

When being powered by a PoE power supply, a PD can also connect to other power supplies for redundant backup of the power supplies.

1.1.2 Power Supply Management for the PoE System

The IEEE 802.3af standard (PoE) specifies the power detection and control items in the remote system, and defines the methods for devices to power VoIP phones, security systems, wireless APs, and other equipment through Ethernet cables. The power provided for devices complying with the IEEE 802.3af standard is less than or equal to 15 W.

Based on compatibility with IEEE 802.3af, the IEEE 802.3at standard (PoE+) delivers a maximum of 30 W through CAT-5 or higher-level cables to meet the power supply requirements of higher-power wireless APs, video phones, video surveillance systems and other equipment.

Based on compatibility with the IEEE 802.3af and IEEE 802.3at standards, the IEEE 802.3bt standard (PoE++) can complete terminal power supply and data transmission with a maximum of 90 W, breaking through the 30 W restriction on PoE+.

You can switch the power supply management mode (the method for allocating power to PDs connected to the PoE device). The PoE device supports the auto mode and energy-saving mode for power supply management.

In auto mode, the system allocates power based on the classes of PDs detected on ports. A PoE device allocates power to PDs of classes 0 to 4 as follows: 15.4 W for Class0, 4 W for Class1, 7 W for Class2, 15.4 W for Class3, and 30 W for Class4. Different from the above power allocation method, 95 W needs to be allocated to a high PoE (HPoE) port although it falls into Class4. In this mode, even if a device of Class3 consumes only 11 W, the PoE device will allocate 15.4 W to the port connecting to this device.

In energy-saving mode, the PoE device dynamically adjusts allocated power based on actual consumption of PDs. In this mode, the PoE device can power more PDs, but the power fluctuation of some PDs may affect the power supply of other PDs. The energy-saving mode is an optional mode of the PoE device. If the device does not support this mode, a corresponding notification will be displayed during configuration. The energy-saving mode is the current default power supply management mode of the device.

In energy-saving mode, the PoE device calculates the power consumption of the system based on the actual power consumption of the PDs. If power consumption of some PDs fluctuates greatly in this mode, overload may occur on the PoE device, which causes damage to the PoE device. The PoE device provides a command for setting the reserved power of the PoE system to ensure that the PoE device always has "rich" power and that the consumed power will not exceed the limit of the PoE device.

The PoE device provides uninterruptible power supply during hot startup. When the system is restarted, PDs that are being powered will not be powered off during hot startup of the PoE device. After the hot startup is completed, the system recovers the status saved in the configuration file.

The PoE device provides the fast power-on function. When the system is restarted due to power failure, the PoE device can continue powering PDs before the restart ends as long as the PoE device is powered on. In addition, the PoE device returns to the state saved in the configuration file during the previous operation, shortening the PD power failure time.

PoE devices usually use the standard IEEE 802.3af and 802.3at in the industry. There are various types of PD devices in the practical application, and it is inevitable to find out some PoE devices not complying to the standards. To meet this end, Ruijie devices provide PoE-compatible commands to support non-standard PoE devices.

1.1.3 Power Supply Management for PoE Ports

You can configure power supply priorities for ports of a PoE device. The priorities are **Critical**, **High**, and **Low** in a descending order. In auto and energy-saving modes, ports with high priorities are powered first. When the system power of the PoE device is insufficient, ports with low priorities are powered off first. The default priorities of all ports are low.

Ports with the same priority are sorted by the port number. A smaller port number indicates a higher priority. For example, the priority of Port 1 is higher than those of Ports 2 and 3.

For ports with the same priority, newly inserted ports do not preempt the power of ports that are being powered. For ports with different priorities, ports with higher priorities can preempt the power of ports with lower priorities.

You can configure the device to manage the power-on/off process of a port based on time ranges. The time range can be configured by the **time-range** command in the global configuration mode.

You can configure the maximum power of a port to restrict the maximum output power of the port. In the auto and energy-saving modes, configuring the maximum power can restrict the maximum output power of ports. When the power of a port is greater than the configured maximum power for 10 seconds, the port is powered off,

the device connected to the port is powered off, a log indicates power overload for the port, and the LED indicator of the port is displayed in yellow. The port is powered on again 10 seconds later. If the power of the port is still greater than the maximum power for 10 seconds, the port will be powered off again. This process repeats constantly.

1.1.4 Auxiliary PoE Power Supply Functions

The PoE standard MIB (RFC3621) provides **pethMainPseUsageThreshold** to set the power alarm threshold of the system.

PoE devices provide the CLI to set this value. The function of this CLI is the same as pethMainPseUsageThreshold MIB, which is setting the power alarm limit of the system. If the pethNotificationControlEnable switch is enabled in the MIB, the MIB receives notifications on the alarm power.

In actual application, whether the system sends trap notifications in case of power change and port power-on/off needs to be controlled. The pethNotificationControlEnable item is provided in the PoE standard MIB RFC3621, which is used to set whether to send trap notifications.

In actual application, you often have to record the PD connected to a specific PoE port. RFC3621 provides pethPsePortType to set the PD description.

PoE devices provide the CLI to set this value.

1.1.5 LLDP Classification

According to the IEEE 802.3at standard, PDs supporting IEEE 802.3at must support both hardware two-event classification (2-Event Physical Layer classification in the standard) and LLDP classification (Data Link Layer classification in the standard). A PD can identify itself as a Class4 type by exchanging LLDP packets with the PSE. The PSE needs to support only one classification.

After a PD of Class4 and Type2 is inserted into a PoE device, the PoE device performs detection and classification first and then supplies power to the PD. The PoE device identifies a device as Type1 device and provides a maximum of 13 W power by default. After LLDP classification is performed, a PD can be identified as a Type2 device. If the PoE device has sufficient power, the PD can obtain a maximum of 25.5 W power. If the PoE device cannot allocate more power any longer, the PD will constantly send LLDP power request packets to request power allocation. The following table lists the maximum power that can be requested by PDs of each class.

Table 1-1 Table of Power Corresponding to Each PD Class

Class	Type	Maximum Power (W)	Allocated Power (W)
Class 0	Type 1	13	15.4
Class 1	Type 1	3.9	4
Class 2	Type 1	6.5	7
Class 3	Type 1	13	15.4
Class 4	Type 1	13	15.4
Class 4	Type 2	25.5	30

Since the cable loss needs to be deducted from the power provided by the PSE, the allocated power is slightly higher than the maximum power requested by the PD. This function is enabled by default and takes effect only in auto mode.

1.1.6 Upgrading the MCU Firmware

Copy the corresponding microcontroller unit (MCU) upgrade package to the TMP directory of the PoE device, and optimize the PoE device by upgrading the MCU firmware to the new version. After the upgrade, the firmware can take effect without restarting the device. When the MCU is upgraded, the PD cannot be powered. Therefore, it is normal for the PD to be powered off during the upgrade. During the upgrade, if the PoE device is restarted due to power failure and other reasons, the MCU will become abnormal and unable to supply power to the PD. You need to upgrade the MCU again to restore the PoE function of the device.

1.1.7 Power Supply Management for PoE Line Cards

You can enable or disable the PoE function of line cards. If the PoE function of a line card is disabled, the line card will not participate in power allocation. You can set the high, medium, and low priorities for line cards. The default priority is low. Power is first allocated to a line card with the high priority. The line card with the high priority can preempt the power of a line card with a lower priority. For the line cards with the same priority, the priority is higher for the line card with a smaller slot ID when the device is started, and the priority is lower for the line card that is inserted later after the device is started. For the same priority, the line cards preempt power according to the slot number and insertion sequence. You can configure allocated power for line cards.

⚠ Caution

For PoE chassis devices with external power supplies, each PoE power supply separately powers the ports on a PoE line card. Therefore, disable the power supply function of a PoE line card.

1.1.8 Protocols and Standards

- IEEE 802.3af
- IEEE 802.3at

1.2 Configuration Task Summary

The PoE configuration includes the following tasks:

(1) Configuring Power Supply of the PoE System

(2) Configuring Power Supply on PoE Ports

(3) Configuring Auxiliary PoE Power Supply Functions

(4) Configuring LLDP Classification

1.3 Configuring Power Supply of the PoE System

1.3.1 Overview

- Configure the PoE mode and change the power allocation mode for PDs. In auto mode, power is allocated based on PD classes. In energy-saving mode, power is allocated based on actual power consumption.
- Configure **poe uninterruptible-power**, which maintains the PoE power supply function during hot startup.

1.3.2 Restrictions and Guidelines

- If the power supply management mode is switched, all PoE ports are powered off and then powered on based on the new power supply management mode. To ensure that the PoE device can power more ports, you can use the energy-saving mode and allocate power to the ports based on actual power consumption.
- In actual application, devices may need to be restarted. For example, after the management software is upgraded, a PoE device needs to be restarted. However, many PDs are normally powered by the PoE device in this case. Direct restart may cause power-off and then power-on of the PDs, that is, the PDs may be interrupted for a period of time.
- If connected PDs do not meet the PoE standard, the function of being compatible with non-standard PDs can be enabled to supply power to the PDs. Running this command for ports not connected to PDs may cause burning of peer devices due to incorrect power-on. Therefore, you need to run this command when PDs are connected to ports.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the power supply management mode.

poe mode { **auto** | **energy-saving** }

The power supply management mode is the energy-saving mode by default.

(4) Configure the uninterruptible power supply during hot startup.

poe uninterruptible-power

After this function is enabled or disabled, the configuration will take effect upon next reset only after being saved.

The uninterruptible power supply during hot startup is disabled by default.

(5) (Optional) Configure the compatibility with non-standard PDs.

poe legacy

The compatibility with non-standard PDs is disabled by default.

(6) Return to the privileged EXEC mode.

end

(7) Save the configuration.

write

1.4 Configuring Power Supply on PoE Ports

1.4.1 Overview

- Configure **poe power-off time-range** to ensure that ports are not powered off within the time range.
- Configure **poe priority**. If the power is insufficient, ports with high priorities can preempt the power of ports

with low priorities but ports with the same priority do not preempt the power from each other.

- Configure **poe max-power** for ports. If the power consumed by a port exceeds 1.1 times the maximum power, the port is powered off. After a penalty period of 10 seconds, the port is powered on again.

1.4.2 Restrictions and Guidelines

- If you run the **interface range** command to configure the PoE function for ports in batches, the enabling or disabling of the PoE function for a port may affect the global power supply management because the range command is configured for ports one after another. Therefore, ports may be powered on and then off during the configuration, which is normal.
- Port-based configuration is supported. The accuracy of the regular power supply function for a PoE port is 1 minute and 30 seconds.
- When *max-power* is set to 0, the port is powered off and not powered on again. The value of *max-power* ranges from 0 to 15.4 for a PoE device that supports IEEE 802.3af only, and from 0 to 95 for an HPoE port. Configure the maximum power of a port. The maximum power cannot exceed 1.1 times the configured power. This reduces the impact of high power consumed by a single port on power management. Configure the maximum power for a port. In static mode, the maximum power configuration of the port does not take effect.

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/disable the power supply control for a port.

poe enable

To enable or disable the PoE function for a port, you must enable or disable the power supply of the port.

By default, the PoE function is enabled for ports of access and aggregation devices and disabled for core devices.

(5) Configure the regular power-off function for a port.

poe power-off time-range *name*

When the power supply function is enabled for a port, the power-on/off of the port is managed based on the period of time specified by ***range-name***.

By default, the regular power-off function is not configured for ports.

(6) Configure power supply priorities for ports.

poe priority { **low** | **high** | **critical** }

In scenarios with insufficient power, you can configure priorities for the ports so that stable power is supplied to some ports. Ports with higher priorities preempt the power of ports with lower priorities. In this case, certain ports with lower priorities may be powered off due to insufficient power.

The power supply management priority of a port is **low** by default.

(7) Configure the maximum power allocated to the port.

poe max-power *max-power*

This command takes effect in auto and energy-saving modes.

The maximum power of a port is not limited by default.

1.5 Configuring Auxiliary PoE Power Supply Functions

1.5.1 Overview

- Configure **poe warning-power** to display a warning when the power used by the system exceeds the alarm threshold.
- Configure **poe notification-control enable** to control whether the system sends trap notifications in case of power change and port power-on/off.
- Configure **poe pd-description** to identify the PD connected to a port.

1.5.2 Restrictions and Guidelines

- Configure the power alarm threshold of the system. When the power used by the system exceeds the threshold, the system displays a warning. If you set the power alarm threshold of the system by using **pethMainPseUsageThreshold** provided by the PoE MIB, the CLI will be configured as well.
- When trap message sending is enabled, trap messages will be sent when the alarm power notification and power on/off notification of the system are enabled or disabled. The command can control only sending of trap messages defined in the RFC3621 and does not take effect for trap messages not defined in the RFC3621. When the trap message sending function defined in the RFC3621 is enabled, a notification is sent if the alarm power changes from being lower than or equal to the system power to being higher than the system power. If the alarm power is always higher than the system power, no trap message will be sent. If the alarm power changes from being higher than or equal to the system power to being lower than the system power, no trap message will be sent if the alarm power is always lower than the system power subsequently.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the power alarm threshold of the system.

poe warning-power *power-threshold*

The power alarm threshold configured for the system is **90** by default.

(4) Configure the trap sending switch of the system.

poe notification-control enable

By default, the system turns off the trap sending switch.

(5) (Optional) Configure the PD descriptor of the port.

poe pd-description *pd-name*

Configure the PD descriptor of the port to easily identify the PD connected to the port. If you set the PD by using **pethPsePortType** provided by the MIB, the CLI will be configured as well.

By default, a port has no PD descriptor.

1.6 Configuring LLDP Classification

1.6.1 Overview

- Configure **poe class-lldp enable** to support power supply and power negotiation through LLDP between a PoE device and PDs.

1.6.2 Restrictions and Guidelines

- The system switches to the energy-saving mode. Enable the LLDP classification function in global configuration mode and verify that there is no **max-power** configuration on the port.
- If the maximum power is configured for the port using the **Max-power** command, the LLDP power adjustment function of the port fails.
- A PoE device does not allow PDs to adjust their priorities through LLDP packets. The port priorities are managed by the PoE device in a unified manner.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Use the LLDP classification function.

poe class-lldp enable: The LLDP two-event classification function of the system is enabled by default.

1.7 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Table 1-2 PoE Monitoring

Command	Purpose
show poe interface	Displays the PoE configuration and status of a specified port.
show poe interfaces	Displays the PoE statuses or configurations of all ports.
show poe powersupply	Displays the power supply status of the current PoE system.

1.8 Configuration Examples

1.8.1 Configuring Power Supply of the PoE System

1. Requirements

- Each of the connected PDs consumes low power, but the number of the connected PDs is large and all ports are occupied.
- The PDs should not be disconnected during hot startup.

2. Notes

- Switch the mode to the energy-saving mode.
- Support uninterruptible power supply during hot startup.

3. Procedure

Create a link aggregation on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# poe mode energy-saving
DeviceA(config)# poe uninterruptible-power
```

Create a link aggregation on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 2/1-2
DeviceB(config-if-range)# port-group 3
```

4. Verification

Run the **show poe powersupply** command to display the configuration and the power supply information.

```
DeviceA# show poe powersupply
Device member                : 1
Power management             : energy-saving
PSE total power              : 125.0 W
PSE total power consumption    : 15.0 W
PSE available power           : 125.0 W
PSE total remain power         : 110.0 W
PSE peak power               : 15.0 W
PSE average power             : 13.9 W
PSE powered port             : 1
PSE disconnect mode           : dc
PSE warning power            : 90
PSE mcu/pse version           : 111/222 (mcu/pse)
PSE class lldp               : enable
PSE uninterruptible-power      : disable
PSE fast on                  : disable
```

1.8.2 Configuring Power Supply on PoE Ports

1. Requirements

- The port GigabitEthernet 0/1 requires a stable power supply not affected by the network environment.
- The port is powered off from 8:00 to 12:00 and powered on in other time.
- The maximum power of the port does not exceed 17 W.

2. Notes

- Set the priority of the port GigabitEthernet 0/1 to **critical**.
- Configure **time-range** and associate the port **time-range** configuration of the PoE.
- Set the maximum power of the port GigabitEthernet 0/1 to 15.4 W.

3. Procedure

Configure LACP on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# time-range poe-time
DeviceA(config-time-range)# periodic daily 8:00 to 12:00
DeviceA(config-time-range)# exit
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# poe power-off time-range poe-time
DeviceA(config-if-GigabitEthernet 0/1)# poe priority critical
DeviceA(config-if-GigabitEthernet 0/1)# poe max-power 15.4
```

4. Verification

Run the **show poe interface** command to view the configuration and the power supply information.

```
DeviceA# show poe interface gigabitEthernet 0/1
Interface             : gi0/1
Power enabled          : enable
Power status           : on
Max power             : 15.4W
Current power          : 14.8 W
Average power          : 14.8 W
Peak power            : 14.8 W
LLDP requested power    : N/A
LLDP allocated power    : N/A
Voltage               : 53.5 V
Current               : 278 mA
PD class              : 4
Trouble cause          : None
Priority              : critical
Legacy                : off
Power-off time-range    : poe-time
Power management       : auto
```

```
4pair status          : normal
```

1.8.3 Configuring Auxiliary PoE Power Supply Functions

1. Requirements

- When the occupied system power exceeds 80%, a warning should be displayed.
- When a port is powered on or off, trap notifications should be sent.
- PDs connected to ports can be identified.

2. Notes

- Set the alarm power threshold of the system to 80%.
- Enable the trap sending switch of the system.
- Set the PD descriptor of the port GigabitEthernet 0/1 to **ap220**.

3. Procedure

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# poe warning-power 80
DeviceA(config)# poe notification-control enable
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# poe pd-description ap220
```

4. Verification

Run the **show running** command to check whether the configuration is correct.

1.8.4 Enabling the LLDP Classification

1. Requirements

Correlate a PD of Class4 with the PSE.

2. Notes

- Enable the LLDP classification.

3. Procedure

Perform the following configuration on Device A:

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# poe class-lldp enable
```

4. Verification

Run the **show poe interface gigabitEthernet** 0/1 command to check whether the load balancing algorithm configured for the AP is correct.

```
DeviceA# show poe interface gigabitEthernet 0/1
Interface            : gi0/1
Power enabled         : enable
```

```
Power status          : on
Max power             : 15.4W
Current power         : 14.8 W
Average power         : 14.8 W
Peak power            : 14.8 W
LLDP requested power   : N/A
LLDP allocated power   : N/A
Voltage               : 53.5 V
Current               : 278 mA
PD class              : 4(Type1)
Trouble cause         : None
Priority              : critical
Legacy                : off
Power-off time-range   : poe-time
Power management       : energy-saving
4pair status          : normal
```

Ethernet Switching Configuration

1. Configuring MAC Address
2. Configuring MAC Loopback
3. Configuring VLAN
4. Configuring MAC VLAN
5. Configuring Protocol-based VLAN
6. Configuring Private VLAN
7. Configuring Super VLAN
8. Configuring Voice VLAN
9. Configuring GVRP
10. Configuring QinQ
11. Configuring STP
12. Configuring ERPS
13. Configuring LLDP

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 Configuration Task Summary 3
1.3 Configuring Static MAC Address Entries 4
1.3.1 Overview 4
1.3.2 Restrictions and Guidelines 4
1.3.3 Procedure 4
1.4 Configuring Filtering MAC Address Entries 4
1.4.1 Overview 4
1.4.2 Procedure 4
1.5 Disabling Dynamic MAC Address Learning 4
1.5.1 Overview 4
1.5.2 Disabling MAC Address Learning in Global Configuration Mode 5
1.5.3 Disabling MAC Address Learning for an Interface 5
1.6 Configuring Upper Limit of Learned MAC Addresses 6
1.6.1 Overview 6
1.6.2 Configuring Upper Limit of MAC Addresses Learned from a VLAN 6

1.7 Configuring Aging Time of Dynamic MAC Address Entries 7
1.8 Enabling MAC Address Flapping Detection and Protection 7
1.8.1 Overview 7
1.8.2 Procedure 7
1.9 Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold 8
1.9.1 Overview 8
1.9.2 Restrictions and Guidelines 8
1.9.3 Procedure 8
1.10 Configuring the Function of MAC Address Entry Change Notification 9
1.10.1 Overview 9
1.10.2 Restrictions and Guidelines 9
1.10.3 Procedure 9
1.11 Monitoring 10
1.12 Configuration Examples 11
1.12.1 Configuring MAC Address Flapping Detection 11
1.12.2 Configuring the Function of MAC Address Change Notification 13

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.

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

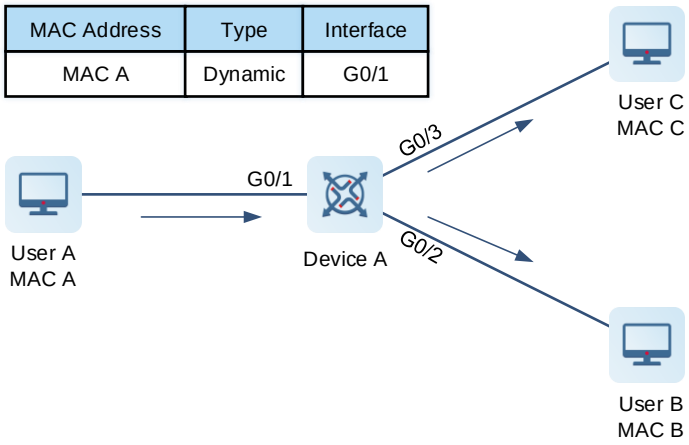
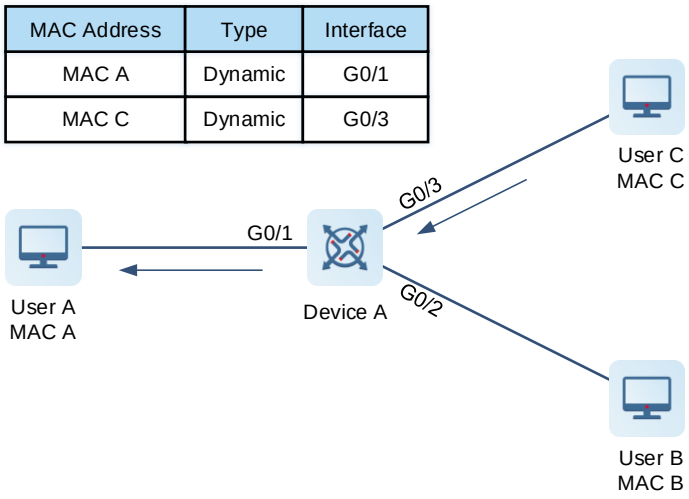


Figure 1-2 Automatically Learning MAC Address Entry II



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 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 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

1.3 Configuring Static MAC Address Entries

1.3.1 Overview

You can manually configure static MAC address entries to bind MAC addresses to device interfaces.

1.3.2 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.

1.3.3 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.

1.4 Configuring Filtering MAC Address Entries

1.4.1 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.

1.4.2 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.

1.5 Disabling Dynamic MAC Address Learning

1.5.1 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.

1.5.2 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.

1.5.3 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 *Configuring IEEE 802.1X*, *Configuring IP Source Guard*, or *Configuring Port Security*.
- 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.6 Configuring Upper Limit of Learned MAC Addresses

1.6.1 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 a VLAN (for example, when it is attacked by packets with different source addresses) and prevent MAC address learning failures on other VLANs. In this case, you can configure the upper limit of MAC addresses learned from each 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 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.

1.6.2 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 { **discard** | **forward** }

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 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.

1.8 Enabling MAC Address Flapping Detection and Protection

1.8.1 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.

1.8.2 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.9 Configuring Reporting Interval of MAC Address Table Usage Alarms and MAC Address Table Usage Threshold

1.9.1 Overview

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 of a device exceeds the upper limit, the device prints an alarm message. When the usage of a MAC address table is lower than the lower limit, the device prints an alarm clearing message.

1.9.2 Restrictions and Guidelines

Each alarm clearing message corresponds to a MAC address table usage alarm message. Only when a MAC address table usage alarm message is printed, an alarm clearing message will be printed if the MAC address usage becomes lower than the lower limit. Even if the MAC address table usage alarm or alarm clearing is triggered multiple times in an alarm period, the corresponding message is printed once.

1.9.3 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*

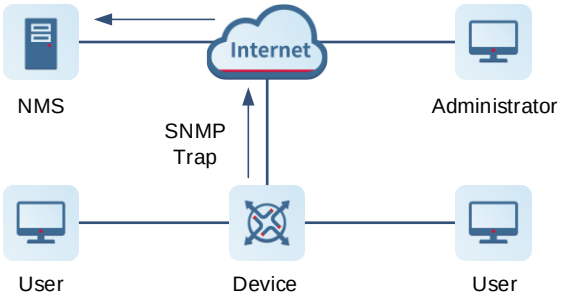
By default, the upper and lower limits for reporting MAC address table usage alarms are 80% and 70%, respectively.

1.10 Configuring the Function of MAC Address Entry Change Notification

1.10.1 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 multiple 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.

1.10.2 Restrictions and Guidelines

A MAC address entry change notification is generated only for a dynamic MAC address entry.

1.10.3 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.11 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 [**address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] | [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]] **show mac-address-table static** [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] **show mac-address-table filtering** [**address** *mac-address*] [**all**] [**vlan** *vlan-id* | **vni** *vni-id* | **vsi** *vsi-id*]	Displays the MAC address table.
show mac-address-table { **evpn** | **mlag** } [**address** *mac-address*] [**all**] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**vni** *vni-id*] [**vsi** *vsi-id*]	Displays the EVPN or MLAG address table.
show mac-address-table [**vni** *vni-id*] [**vsi** *vsi-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 interface *interface-type interface-number* [**vlan** *vlan-id*] [**all**]	Displays static or dynamic MAC address entries for a specified interface
show mac-address-table max-dynamic-mac-count vlan [*vlan-id*]	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.

1.12 Configuration Examples

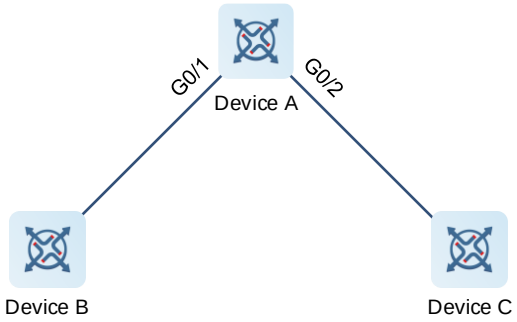
1.12.1 Configuring MAC Address Flapping Detection

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 Topology of 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-if-GigabitEthernet 0/1)# mac-address-table flapping action error-down
DeviceA(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-if-GigabitEthernet 0/2)# mac-address-table flapping action error-down
DeviceA(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
!
```

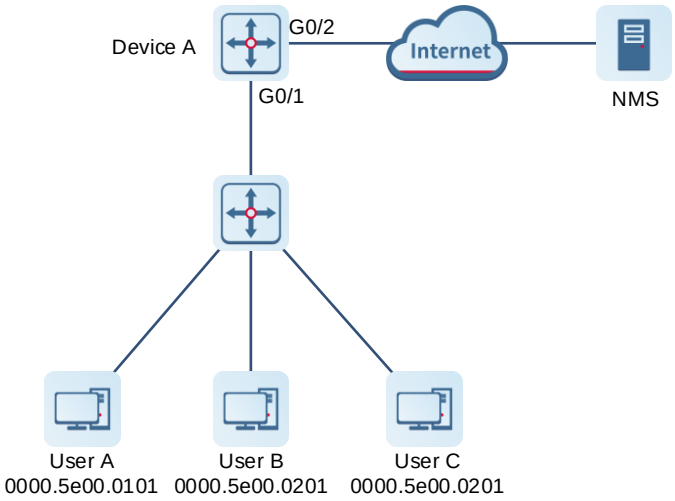
1.12.2 Configuring the Function of MAC Address Change Notification

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 Topology of MAC Address 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

- View the global configuration information about the function of MAC address change notification.
- Check whether an interface is enabled with the function of MAC address change notification.
- View the MAC address table of an interface and run the **clear mac-address-table dynamic** command to simulate the aging of dynamic addresses.
- View the global configuration information about the function of MAC address change notification. View the history table of MAC address change notifications.

Run the **show mac-address-table notification** command to check whether the NMS can normally receive MAC address change notifications. The command can be executed in privileged EXEC mode, global configuration mode, and interface configuration mode. The Interval(Sec) field specifies the notification interval, Maximum History Size specifies the maximum number of entries in the history table of MAC address change notifications, and Current History Size indicates the current number of entries in the history table.

```
DeviceA# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

Run the **show mac-address-table notification** command to view the history table of MAC address change notifications.

```
DeviceA # show mac-address-table notification interface gigabitethernet 0/1
Interface             MAC Added Trap    MAC Removed Trap
-----------           --------------    --------------
GigabitEthernet 0/2   Enabled          Enabled
DeviceA # show mac-address-table interface GigabitEthernet 0/1
Vlan       MAC Address         Type    Interface
----------  -------------------- -------- -------------------
  1       00d0.3232.0001      DYNAMIC  GigabitEthernet 0/1
DeviceA # show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 1
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 Restrictions and Guidelines 1

1.3 Configuring Basic Features 1

1.3.1 Overview 1

1.3.2 Procedure 1

1.4 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 Restrictions and Guidelines

- MAC loopback can only enabled on a physical port instead of a logical interface.
- The function supports working on a Layer 2 or Layer 3 Ethernet interface.

1.3 Configuring Basic Features

1.3.1 Overview

This section describes how to enable MAC loopback on an interface for interface self-loop.

1.3.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-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.

1.4 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 interfaces enabled with MAC loopback.

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....2
1.1.5 VLAN Frame Processing Rules....3
1.1.6 Intra-VLAN Communication on One Device....4
1.1.7 Intra-VLAN Communication Across Devices....8
1.1.8 Inter-VLAN Communication....9
1.1.9 VLAN Assignment Methods....14
1.1.10 Protocols and Standards....15
1.2 Restrictions and Guidelines....15
1.3 Configuration Task Summary....15
1.4 Configuring VLANs....16
1.4.1 Overview....16
1.4.2 Configuration Tasks....16
1.4.3 Creating and Configuring VLANs....16
1.4.4 Configuring VLAN Names....17
1.4.5 Configuring SVIs....17
1.5 Configuring Access Ports....18
1.5.1 Overview....18

1.5.2 Restrictions and Guidelines 18
1.5.3 Procedure (Interface Configuration Mode) 18
1.5.4 Procedure (VLAN Configuration Mode) 19
1.6 Configuring Trunk Ports 20
1.6.1 Overview 20
1.6.2 Restrictions and Guidelines 20
1.6.3 Procedure 20
1.7 Configuring Uplink Ports 21
1.7.1 Overview 21
1.7.2 Restrictions and Guidelines 21
1.7.3 Procedure 22
1.8 Configuring Hybrid Ports 23
1.8.1 Overview 23
1.8.2 Restrictions and Guidelines 23
1.8.3 Procedure 23
1.9 Monitoring 24
1.10 Configuration Examples 25
1.10.1 Configuring Layer 2 Isolation and Layer 3 Interconnection of VLANs 25

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 in Layer 2. Devices on different VLANs can implement communication through Layer 3 devices or Layer 3 interfaces.

1.1.2 Background and Functions

1. Background

The early 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. The working mode will lead to two problems:

- If the network scale is enlarged, the increasing broadcast packets waste bandwidth.
- As packets in a LAN are broadcast, each STA in the broadcast domain can receive broadcast packets in the entire LAN. If users obtain these packets using a packet capture tool, the content in the packets may be intercepted, which affects information security.

Use routers to solve the preceding two problems. Routers communicate based on Layer 3 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). In contrast, a VLAN is a solution with lower cost and solves the preceding problems by dividing the physical LAN into multiple logical LANs.

2. Functions

- Layer 2 isolation

  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. 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 Layer 3 interface interconnected with VLANs is configured, 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.

- Layer 3 interconnection

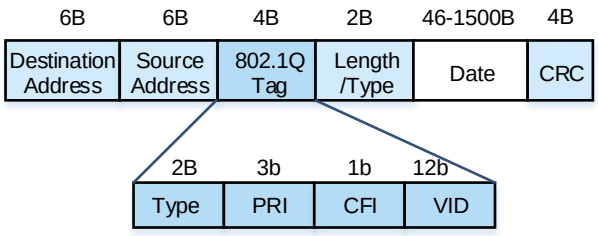
To realize Layer 3 communication between VLANs, a virtual interface is developed for an Layer 3 switch, based on the concept of router subinterfaces. The virtual interface is referred to as Switch Virtual Interface (SVI). In a Layer 3 switch, you can create an SVI and an SVI IP address for each VLAN. The SVI functions as a VLAN gateway to implement Layer 3 communication between VLANs. Therefore, an SVI is also referred to as a VLAN interface.

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 1-1. 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 of a VLAN ID is from 1 to 4094. The value **0** and **4095** are reserved and unusable.

Figure 1-1 802.1Q Frame Format



1.1.4 Port Types and Link Types

Interfaces can be classified into L2 interfaces and Layer 3 interfaces. Only L2 interfaces can be added to VLANs. Table 1-1 lists basic types of L2 interfaces. You can configure the L2 interface type of an interface to determine the allowed VLANs of the interface, and whether the packets forwarded by the interface are tagged.

Table 1-1 Basic Types of L2 Interfaces

Port Type	Function
Access	An access port carries traffic for only one VLAN. Only frames from this VLAN can pass the port. This VLAN is referred to as access VLAN, which owns attributes of a native VLAN and an allowed VLAN. 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.

Port Type	Function
Trunk	A trunk port carries traffic for one native VLAN and multiple allowed 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.
Uplink	An uplink port carries traffic for one native VLAN and multiple allowed 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 *Configuring QinQ*.
Hybrid	A hybrid port carries traffic for one native VLAN and multiple allowed VLANs. Allowed VLANs are classified into tagged VLANs and untagged 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 downlink clients in MAC VLAN scenarios. For more information, see *Configuring MAC VLAN*.

VLAN links include access links and trunk links.

- An access link connects STAs to a switch interface. Although some STAs can identify frames that carry VLAN tags, most STAs cannot do so. Generally, a port transmits untagged frames in the access link to ensure the compatibility of different STAs.
- 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. Untagged frames and tagged frames are transmitted based on different types of ports. Ensure that the native VLAN configuration on the peer device is consistent with that on the local device so that the trunk port transmits untagged frames from the native VLAN and tagged frames from other allowed VLANs,

Access ports can be connected by an access link only. Hybrid ports can be connected by both an access link and a trunk link. Trunk ports and uplink ports can be connected by a trunk link only.

1.1.5 VLAN Frame Processing Rules

- Frame receiving rule

  When detecting an incoming untagged frame, the port regards that the frame comes from the native VLAN of the port. If the native VLAN is an allowed VLAN of the port, the port receives the packet, and identifies the frame as one from the native VLAN. Otherwise, the port discards the packet.

  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 Layer 3 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).

The following example displays actual application of the above rules. Table 1-2 shows the interfaces and configurations in the example.

Table 1-2 Interface Examples

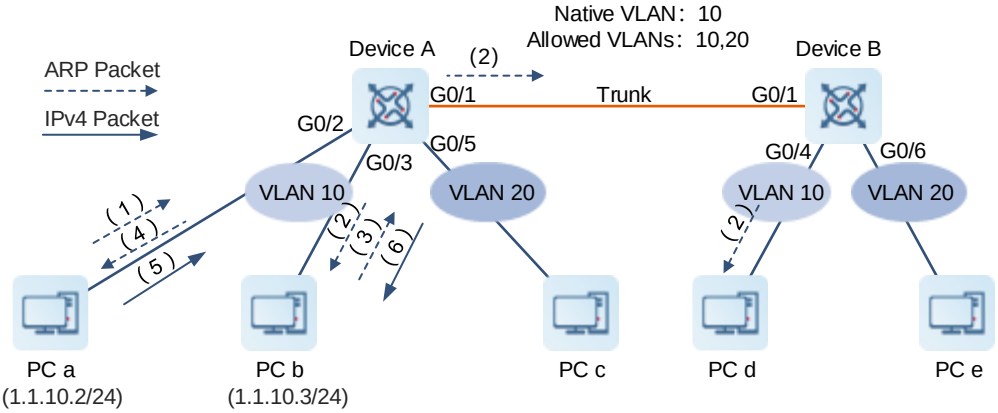
Interface	Mode	Native VLAN	Allowed VLAN
GigabitEthernet 0/1	Access	10	10 (Untagged)
GigabitEthernet 0/2	Trunk	10	10 (Untagged), 20 (Tagged), and 30 (Tagged)
GigabitEthernetGi 0/3	Hybrid	20	20 (Untagged), 10 (Tagged), and 30 (Tagged)
GigabitEthernetGi 0/4	Uplink	30	30 (Tagged) and 20 (Tagged)

When GigabitEthernet 0/1 receives an untagged frame or a frame with a VLAN 10 tag, it forwards the frame to GigabitEthernet 0/2 and GigabitEthernet 0/3 that allow VLAN 10. The VLAN 10 frame sent to GigabitEthernet 0/2 is untagged, and the VLAN 10 frame sent to GigabitEthernet 0/3 is tagged. When GigabitEthernet 0/4 receives an untagged frame or a frame with a VLAN 30 tag, it forwards the frame to GigabitEthernet 0/2 and GigabitEthernet 0/3 that allow VLAN 30. The VLAN 30 frame sent to GigabitEthernet 0/2 is tagged, and the VLAN 30 frame sent to GigabitEthernet 0/3 is untagged.

1.1.6 Intra-VLAN Communication on One Device

As shown in the topology in Figure 1-2, Device A and Device B are connected through the trunk port GigabitEthernet 0/1. PC a and PC b are connected to VLAN 10 through device A. The communication between PC a and PC b is intra-VLAN communication on one device.

Figure 1-2 An Example of Intra-VLAN Communication Within One Device



Through IP addresses, PC a (1.1.10.2/24) first determines that PC b (1.1.10.3/24) is in the same subnet as the device. The device uses the MAC address of PC b as the destination MAC address for communication. The communication steps are as follows:

If PC a does not find the MAC address of PC b, the communication goes from step (1); if PC a finds the MAC address of PC b, the communication goes from step (5).

(1) PC a does not find the MAC address of PC b in the Address Resolution Protocol (ARP) table. PC a sends a broadcast ARP request packet to request the MAC address of PC b. Device A learns the MAC address of PC a through the ARP request packet.

(2) Device A forwards the broadcast ARP request packet. PC b learns the MAC address of PC a through the ARP request packet.

(3) PC b sends a unicast ARP reply packet to PC a. Device A learns the MAC address of PC b through the ARP reply packet.

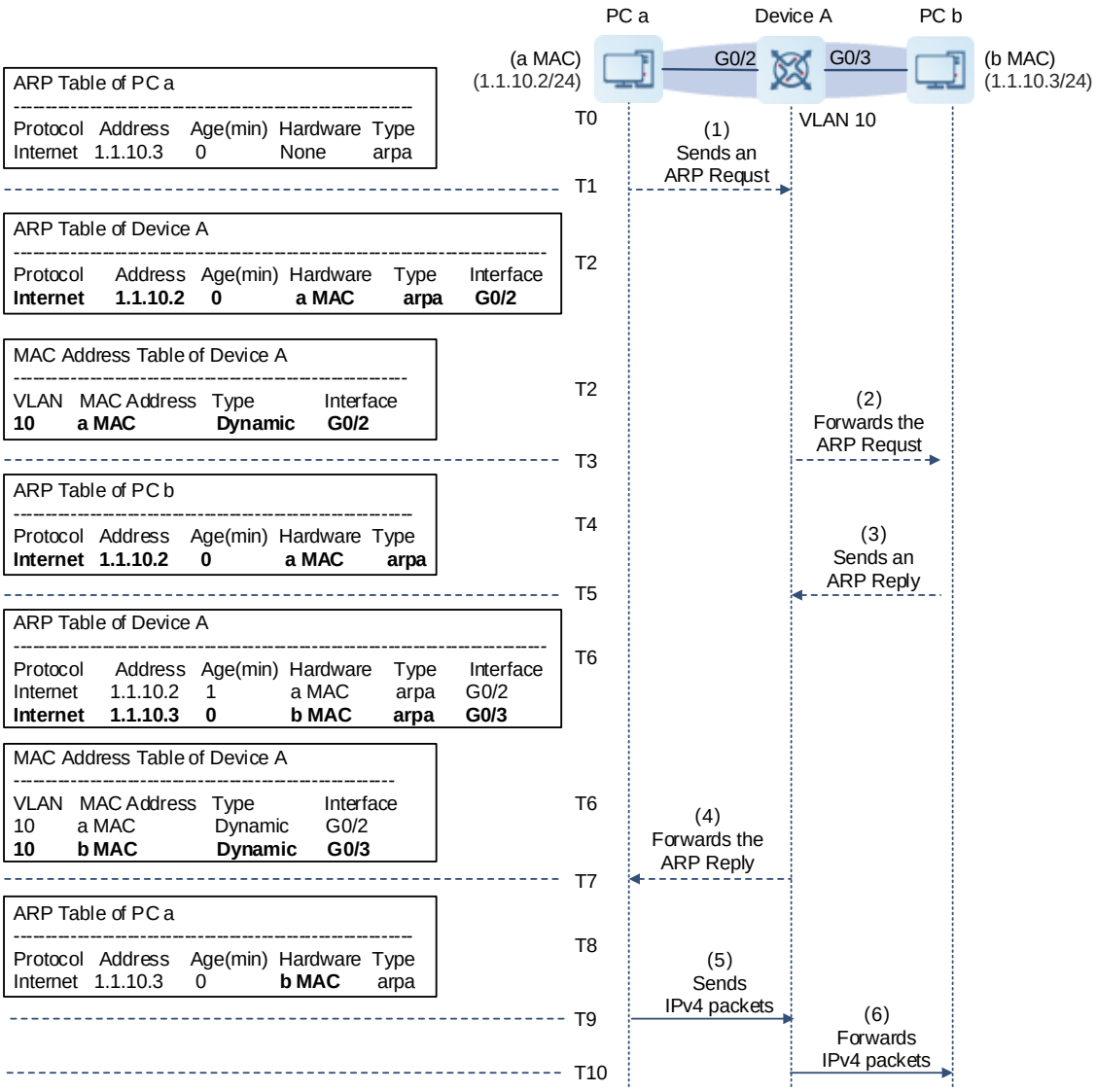
(4) Device A finds the MAC address of PC a in the ARP table and forwards the unicast ARP reply packet. PC a learns the MAC address of PC b through the ARP reply packet.

(5) PC a finds the MAC address of PC b (destination MAC address) in the ARP table and sends a unicast IPv4 packet to PC b.

(6) Device A finds the MAC address of PC b in the ARP table and forwards the unicast IPv4 packet.

Steps of intra-VLAN communication on one device are shown in Figure 1-3.

Figure 1-3 Steps of Intra-VLAN Communication

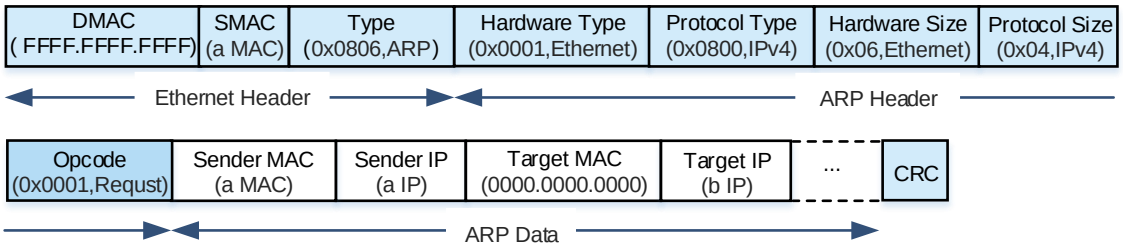


(1) PC a sends an ARP request packet to request the MAC address of PC b.

a. If PC a does not find the MAC address of PC b as shown in T0 in Figure 1-3, PC a sends an ARP request packet encapsulated in an Ethernet broadcast frame (as shown in Figure 1-4) to PC b as shown in T1 in Figure 1-3.

b. Upon receiving the ARP request packet of PC a from GigabitEthernet 0/2, 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. Device A enters the mapping among the IP address, MAC address, port, and VLAN of PC a into the ARP table and enters the mapping among the VLAN, MAC address and port of PC a into the dynamic MAC address table, as shown in T2 in Figure 1-3.

Figure 1-4 The ARP Request Packet Sent by PC a for Requesting the MAC Address of PC b



(2) Device A forwards the ARP request packet.

a. Device A searches for the port that allows VLAN 10, and broadcasts the ARP request to GigabitEthernet 0/1 and GigabitEthernet 0/3 except the source port GigabitEthernet 0/2, as shown in T3 in Figure 1-3.

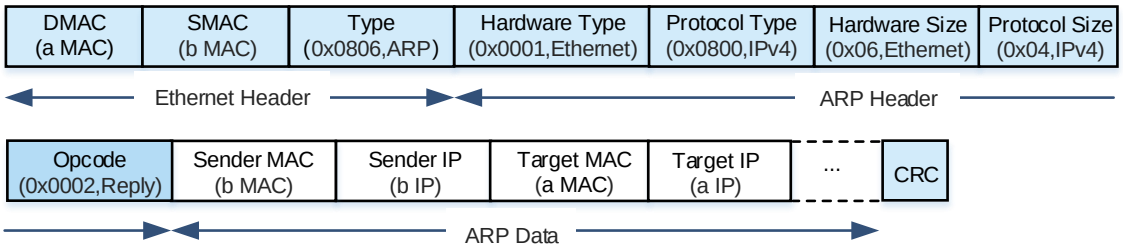
b. PC b receives the ARP request (as shown in Figure 1-4) of PC a from GigabitEthernet 0/3, learns the mapping between the IP address and MAC address of PC a, and enters the mapping into the ARP table.

(3) PC b sends a unicast ARP reply packet.

a. PC b finds that the destination IP address in the ARP request matches its own IP address, it sends a unicast ARP reply (as shown in Figure 1-5) to PC a, as shown in PC b in T5 in Figure 1-3.

b. Upon receiving the ARP reply of PC b from GigabitEthernet 0/3, Device A learns the source IP address. Device A enters the mapping among the IP address, MAC address, port, and VLAN of PC b into the ARP table and enters the mapping among the VLAN, MAC address and port of PC b into the dynamic MAC address table, as shown in T6 in Figure 1-3.

Figure 1-5 The ARP Reply Packet Sent by PC b to PC a



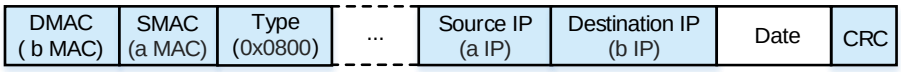
(4) Device A forwards the ARP reply packet.

a. Device A queries the MAC address table, matches MAC address of PC a, and forwards the ARP reply of PC b to GigabitEthernet 0/2, as shown in T7 in Figure 1-3.

b. 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, as shown in T8 in Figure 1-3.

PC a sends an IPv4 packet.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 (as shown in Figure 1-6) to PC b, as shown in T9 in Figure 1-3 .

Figure 1-6 The IPv4 Packet Sent from PC a to PC b



(5) Device A forwards the IPv4 packet.

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 and matches the destination MAC address of PC b, and forwards the packet (as shown in Figure 1-6) to GigabitEthernet 0/3, as shown in T10 in Figure 1-3.

1.1.7 Intra-VLAN Communication Across Devices

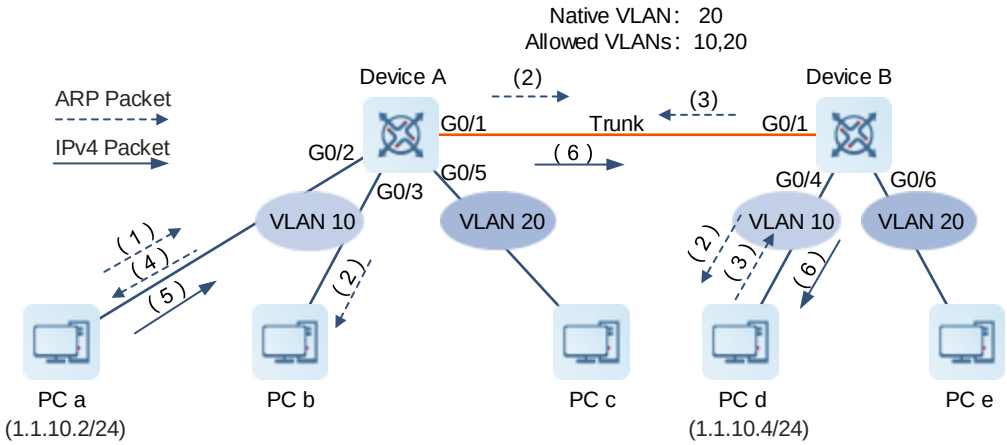
Ports on different devices can be assigned to the same VLAN. The procedure of intra-VLAN communication across devices is similar to the procedure of intra-VLAN communication on one device, except for the following:

- The trunk port sends a packet. If the packet comes from the native VLAN, the packet is untagged. Otherwise, the packet is tagged.
- When receiving a packet, the trunk port determines that the packet comes from the native VLAN if it is untagged. If the native VLAN is an allowed VLAN of the port, the packet is allowed to pass through the port. Otherwise, the packet is not allowed to pass through the port. If the packet is tagged, the port check whether the packet comes from an allowed VLAN. If yes, the port receives the packet and forwards it. If not, the port discards the packet.

As shown in Figure 1-9, Device A and Device B is connected through the trunk port GigabitEthernet 0/1. PC a is connected to VLAN 10 through Device A, and PC d is connected to VLAN 10 through Device B. The communication between PC a and PC d is intra-VLAN communication across devices.

To explain the process of adding and removing a tag, assume that VLAN 20 is the native VLAN of GigabitEthernet 0/1.

Figure 1-7 An Example of Intra-VLAN Communication Across Devices



PC a determines that PC d is on the same network segment as the device. PC a needs to use the MAC address of PC d as the destination MAC address for communication. The communication steps are as follows:

(1) PC a does not find the MAC address of PC d (the destination MAC address) in the ARP table. PC a sends a broadcast ARP request packet to request the MAC address of PC d. Device A learns the MAC address of PC a through the ARP request packet.

(2) Device A forwards the broadcast ARP request packet. As VLAN 10 is not the native VLAN of the trunk port GigabitEthernet 0/1, add a VLAN 10 tag to the packet and send the packet. When the GigabitEthernet 0/1 port of Device B receives the packet, the port finds that the packet carries a VLAN 10 tag and VLAN 10 is an allowed VLAN. The port allows the packet to pass through. The port removes the VLAN 10 tag from the packet and forwards the ARP request packet to the GigabitEthernet 0/4 port. Device B and PC d learn the MAC address of PC a through the ARP request packet.

(3) PC d sends a unicast ARP reply packet. The GigabitEthernet 0/1 port of Device B adds a VLAN tag to the ARP reply packet and forwards the packet. Device B and Device A learn the MAC address of PC d through the ARP reply packet.

(4) When the GigabitEthernet 0/1 port of Device A receives the packet, the port finds that the packet carries a VLAN 10 tag and VLAN 10 is an allowed VLAN. The port allows the packet to pass through. Device A queries the ARP table and matches the MAC address of PC a. The port removes the VLAN 10 tag from the packet and forwards the unicast ARP request packet to the GigabitEthernet 0/2 port.

(5) PC a finds the MAC address of PC d (the destination MAC address) in the ARP table and sends a unicast IPv4 packet to PC d.

(6) Device A queries the ARP table, matches the MAC address of PC d, adds a VLAN 10 tag to the IPv4 packet and forwards the packet. When receiving the packet, .Device B queries the ARP table, matches the MAC address of PC d, removes the VLAN 10 tag from the IPv4 packet and forwards the packet.

1.1.8 Inter-VLAN Communication

In practice, devices from different VLANs may need to communicate with each other. Although VLAN broadcast domains are isolated in Layer 2, the devices from different VLANs can communicate with each other by using a Layer 3 device. But this method requires routed ports. To address this problem, a routing module can be added to a Layer 2 switch to form a Layer 3 switch.

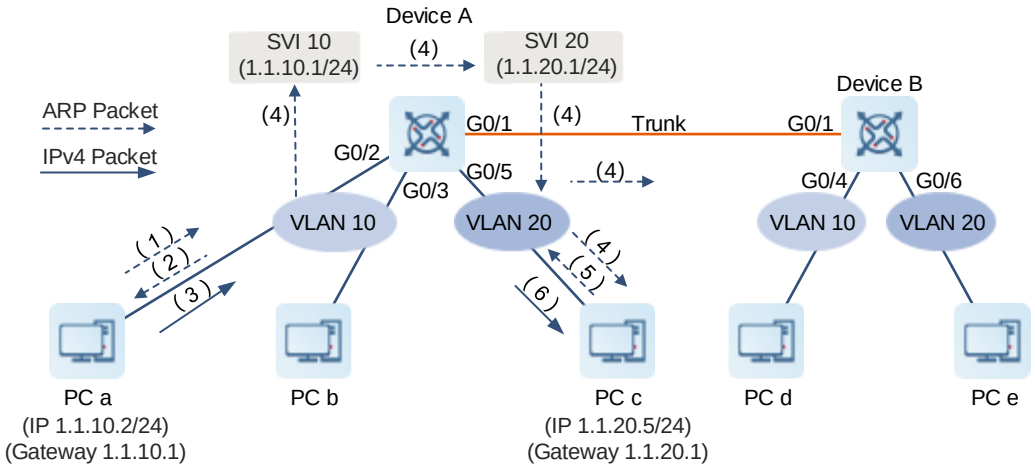
On a Layer 3 switch, one VLAN corresponds to one SVI. The Layer 3 switch takes the SVI as an independent interface, creates an ARP entry for the interface, and records the mapping between the IP address and MAC address of the SVI.

An 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 to be used as the destination MAC address, and then forwards a packet to the gateway.

When the Layer 3 switch receives the packet whose MAC address matches the SVI, the switch enables Layer 3 forwarding. If the Layer 3 switch does not know the MAC address of the destination host, the Layer 3 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 Layer 3 switch learns the IP address, MAC address, port, and VLAN of the destination host, updates the Layer 3 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 Layer 3 switch receives packets with the same destination MAC address, the Layer 3 switch directly queries the Layer 3 routing table, replaces the source and destination MAC addresses, and forwards the packets.

As shown in Figure 1-8, PC a belongs to VLAN 10 and PC c belongs to VLAN 20. They communicate with each other across the VLANs.

Figure 1-8 An Example of Inter-VLAN Communication



After an SVI is created, Device A generates the mappings of IP addresses to MAC addresses and a directly connected route to the Layer 3 SVI. As shown in T0 in Figure 1-9, the gateway MAC address is the MAC address of Device A.

The IP address of PC a is 1.1.10.2/24 and its corresponding gateway IP address is 1.1.10.1/24. The IP address of PC c is 1.1.20.5/24 and its corresponding gateway IP address is 1.1.20.1/24. To communicate with PC c, PC a first determines that they are on different network segments. PC a takes the gateway MAC address as the destination address for communication. The communication steps are as follows:

PC a queries the ARP table for the gateway MAC address corresponding to the gateway IP address (1.1.10.1/24). If PC a does not find the MAC address of the gateway, goes from step (1). If PC a finds the MAC address of the gateway, goes from step (3).

(1) PC a does not find the MAC address of the gateway, it sends a broadcast ARP request packet to request the MAC address of the gateway. Device A learns the MAC address of PC a through the ARP request packet.

(2) Device A sends a unicast ARP reply packet. PC a learns the MAC address of the gateway through the ARP reply packet.

(3) PC a finds the MAC address of the gateway of in the ARP table, uses the gateway MAC address as the destination MAC address, and the IP address of PC c as the destination IP address, and sends a unicast IPv4 packet to PC c. When receiving the packet, if Device A does not find the MAC address of PC c, it performs step (4). If Device A finds the MAC address of PC c, it performs step (6) directly.

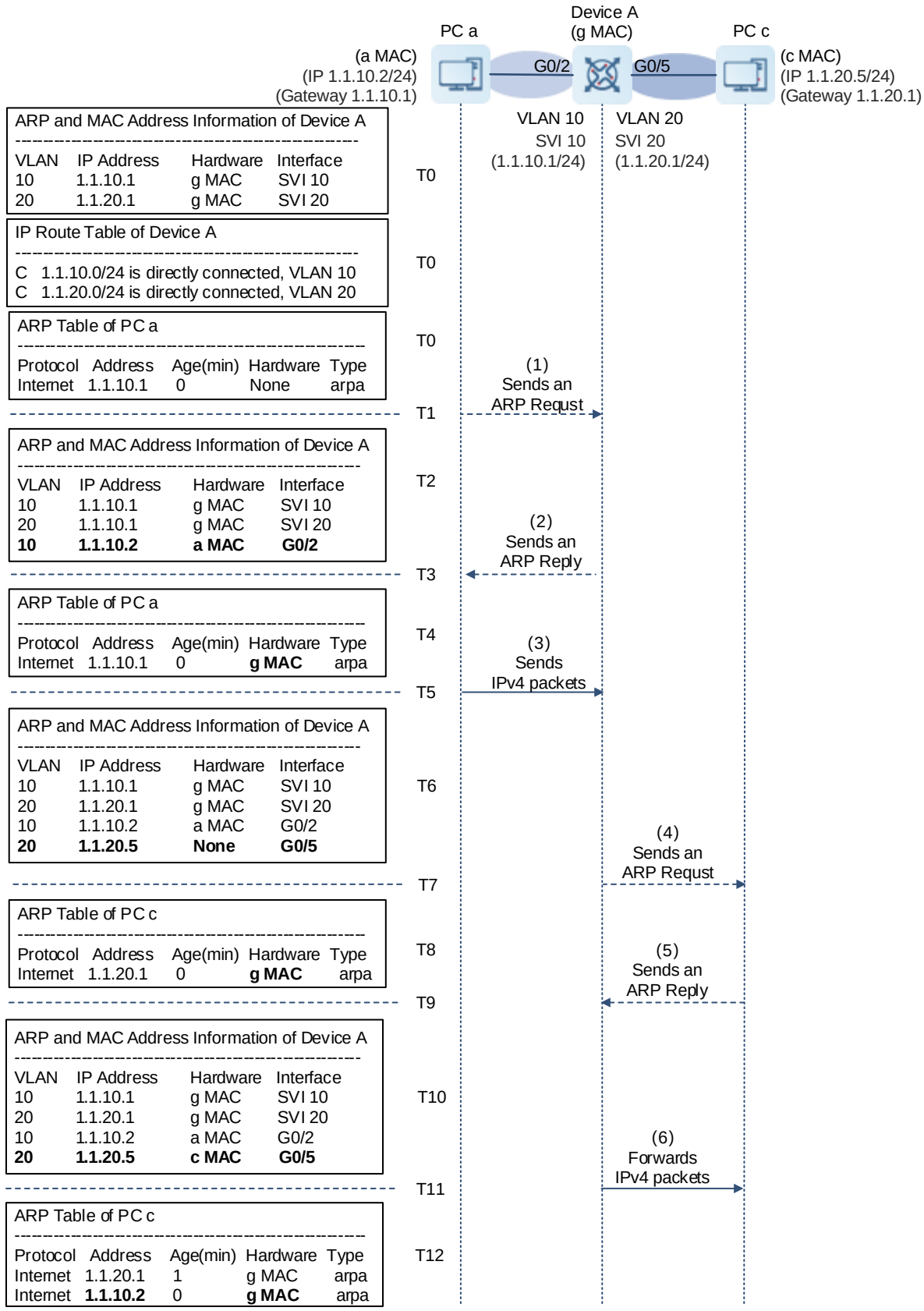
(4) Device A identifies that the destination MAC address is the MAC address of the gateway, and sends the packet to SVI 10 for forwarding. The CPU queries the software routing table, and finds that the egress VLAN corresponding to the destination IP address of PC c is VLAN 20 through the directly connected route of Layer 3 SVIs. SVI 20 in VLAN 20 sends a broadcast ARP request to request the MAC address corresponding to the IP address of PC c. PC c learns the mapping of the MAC address of the gateway and the IP address of SVI 20 through the packet.

(5) PC c sends a unicast ARP reply. Device A learns the MAC address of PC c.

(6) For the packet sent from PC a to PC c, Device A changes its source MAC address from a MAC to g MAC, and changes its destination MAC address from g MAC to c MAC, and then forwards it. PC c learns the mapping of the MAC address of the gateway and the IP address of PC a through the packet.

Steps of inter-VLAN communication are shown in Figure 1-9.

Figure 1-9 Steps of Inter-VLAN Communication

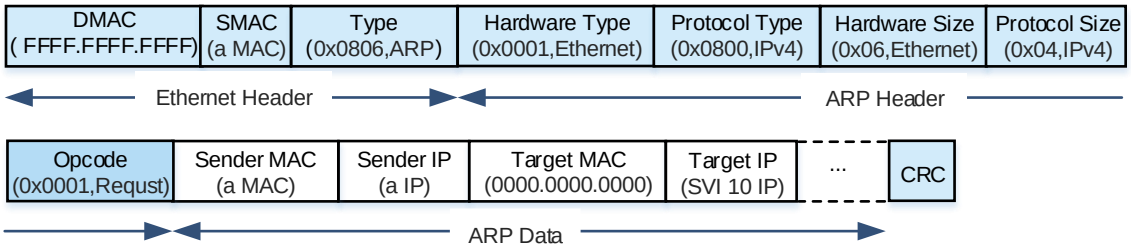


(7) PC a sends an ARP request packet to request the MAC address of the gateway.

a. If PC a does not find the MAC address of the gateway IP address (1.1.10.1) as shown in T0 in Figure 1-9, PC a sends an ARP request packet encapsulated in an Ethernet broadcast frame (as shown in Figure 1-10) to the gateway as shown in T1 in Figure 1-9. The gateway of PC a is SVI 10 whose IP address is 1.1.10.1/24. Therefore, the gateway uses the IP address of SVI 10 as a target IP address.

b. When receiving the ARP request packet of PC a from GigabitEthernet 0/2, 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. Device A enters the mapping among the VLAN, MAC address, and port of PC a into the dynamic MAC address table. The ARP table and the MAC address table contain information about Layer 3 forwarding and such information is called as a Layer 3 routing table, as shown in T2 in Figure 1-9. The routing table cannot be queried but its content is reflected in the ARP table and MAC address table.

Figure 1-10 The ARP Request Packet Sent from PC a for the MAC Address of the Gateway

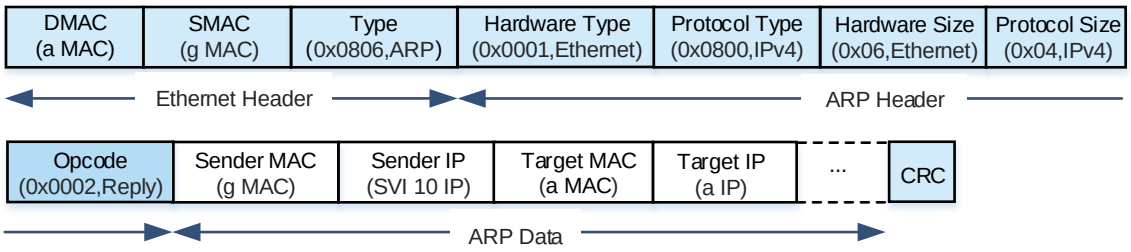


(8) Device A sends an ARP reply packet.

a. 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 10 of this device, it returns a unicast ARP reply and forwards the reply packet through GigabitEthernet 0/2, as shown in T3 in Figure 1-11Figure 1-9. The reply packet (as shown in Figure 1-11) includes the IP address and MAC address of SVI 10.

b. Upon receiving the ARP reply, PC a learns the MAC address corresponding to the gateway IP address of the SVI 10 and updates the ARP table of PC a, as shown in T4 in Figure 1-9.

Figure 1-11 ARP Reply Packet Sent by the Gateway to PC a

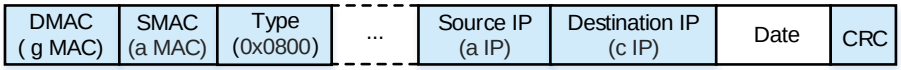


(9) PC a sends an IP packet to PC c.

a. 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 1-12), and forwards the packet to the gateway, as shown in T5 in Figure 1-11Figure 1-9.

b. Upon receiving the packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-12), Device A finds that the packet is untagged. Device A determines that the packet comes from VLAN 10 and updates the MAC address entry of PC a. The destination MAC address (gateway MAC address) is the gateway MAC address of the local device. Therefore, the packet must be forwarded at Layer 3. If Device A finds the MAC address of PC c corresponding to the IP address of PC c, the device goes to step (6).

Figure 1-12 IPv4 Packet Sent by PC a to PC c



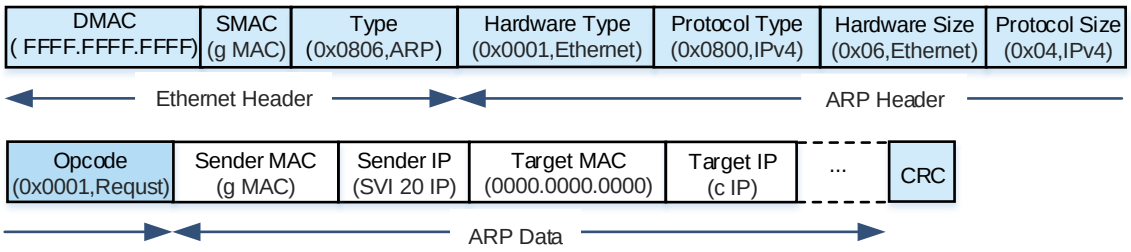
(10) The gateway sends an ARP request for the MAC address of PC c.

a. If Device A does not find the MAC address corresponding to the IP address of PC c (1.1.20.5), it sends the packet to SVI 10 to forward the packet to the CPU.

b. The CPU queries the software routing table, and finds that the IP address matches a direct route to 1.1.20.0/24 and the egress VLAN is VLAN 20. In the egress VLAN (VLAN 20), SVI 20 sends a broadcast ARP request packet for the MAC address of PC c, as shown in T7 in Figure 1-11Figure 1-9. The gateway of PC c is SVI 20. Therefore the gateway uses the IP address of SVI 20, 1.1.20.1/24, as its IP address.

c. The ARP request is sent from GigabitEthernet 0/1 and GigabitEthernet 0/5 that allow VLAN 20. PC c receives the ARP request (as shown in Figure 1-13) 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, as shown in T8 in Figure 1-11Figure 1-9.

Figure 1-13 ARP Request Packet Sent by the Gateway for Requesting MAC Address of PC c

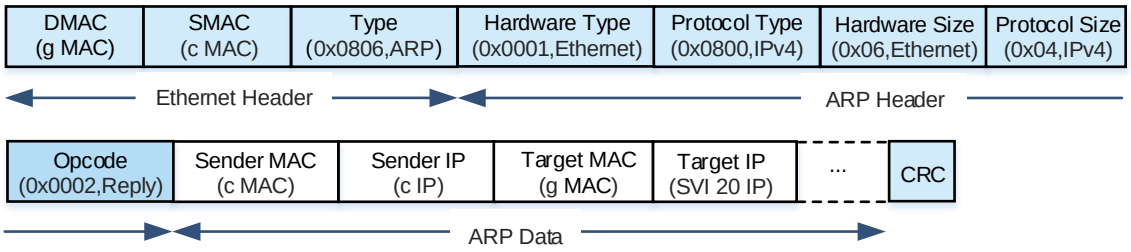


(11) PC c sends an ARP reply packet.

a. 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 1-14), as shown in T9 in Figure 1-11Figure 1-9.

b. Upon receiving the ARP reply (as shown in Figure 1-14) 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, as shown in T10 in Figure 1-11Figure 1-9.

Figure 1-14 ARP Reply Packet Sent by PC c to the Gateway

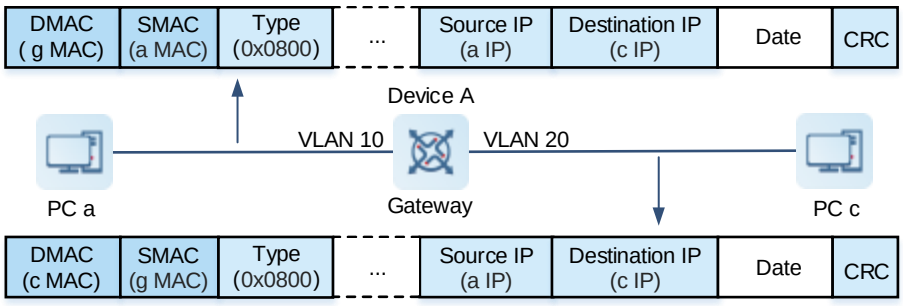


(12) The gateway forwards the IP packet.

a. If Device A finds the MAC address of PC c in the routing table, 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 1-15), as shown in T11 in Figure 1-11Figure 1-9.

b. PC c receives this packet (as shown in Figure 1-15) 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, as shown in T12 in Figure 1-11Figure 1-9. 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 (1.1.10.2), and encapsulates the packet for PC a by using the gateway MAC address as the destination MAC address.

Figure 1-15 Packet Forwarded by the Gateway



1.1.9 VLAN Assignment Methods

1. Port-based Assignment

- Port-based VLAN

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*.

2. Packet-based Assignment

- MAC-based VLAN

MAC-based VLAN is a VLAN assignment method based on MAC addresses. 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. For more information, see *MAC VLAN*.

Usually, MAC-based VLAN is used with the 802.1x VLAN delivery function to ensure secure and flexible access of 802.1x STAs.

- 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-based VLAN

Protocol-based 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-based VLAN assignment. For more information, see *Protocol-based VLAN*.

1.1.10 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 a port to a VLAN, ensure that the port is a Layer 2 interface.
- Run the **show interface switchport** command to show the port type. If the **Switchport** field corresponding to the port is set to **enabled**, the port is a Layer 2 interface. Otherwise, the port is a Layer 3 interface.
- Run the **switchport** command to configure a port as a Layer 2 interface. Run the **no switchport mode** command to restore the default configuration of the Layer 2 interface mode. Then run the **no switchport** command to configure the Layer 2 interface as a Layer 3 interface. When you configure a port as a Layer 2 or Layer 3 interface, all attributes of the interface are restored to the default values in the corresponding interface mode.

1.3 Configuration Task Summary

VLAN configuration includes the following tasks:

(1) Configuring VLANs

- Creating and Configuring VLANs
- (Optional) Configuring VLAN Names
- (Optional) Configuring SVIs

(2) Configure a port type and add ports to a VLAN. Configure at least one of the following tasks.

- Configuring Access Ports
- Configuring Trunk Ports
- Configuring Uplink Ports
- Configuring Hybrid Ports
-

1.4 Configuring VLANs

1.4.1 Overview

Create a VLAN, and enter the VLAN configuration mode.

1.4.2 Configuration Tasks

VLAN configuration includes the following tasks:

(1) Creating and Configuring VLANs

(2) (Optional) Configuring VLAN Names

(3) (Optional) Configuring SVIs

1.4.3 Creating and Configuring VLANs

1. Overview

Create a VLAN, and 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

- When you create a VLAN, the system will prompt the VLAN creation failure if hardware resource is insufficient.
- Run the **no vlan** *vlan-id* command to delete a common static 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.
- Check created VLANs 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.

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*

Only VLAN 1 exists by default.

1.4.4 Configuring VLAN Names

1. Overview

Name a VLAN.

2. Restrictions and Guidelines

- You cannot rename a VLAN the same as the default name of another VLAN.
- You are advised to run the **show vlan** command to check all VLAN names in case of name duplication before you name a VLAN.
- A VLAN is named as VLAN*vlan-id*. For example, the name of VLAN 2 is VLAN0002.
- To restore the VLAN name to a default value, run the **no name** command.

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 VLAN name.

name *vlan-name*

The name of a VLAN is VLAN *vlan-id* by default.

1.4.5 Configuring SVIs

1. Overview

You can create an 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 Layer 3.

2. Restrictions and Guidelines

- You cannot create SVIs for sub-VLANs of a super VLAN or secondary VLANs of a private VLAN.
- In the **interface vlan** *interface-number* command, *interface-number* indicates the SVI ID. An SVI ID must follow the ID of the corresponding VLAN, which ranges from 1 to 4,094.
- To delete a VLAN with a created SVI, run the **no interface vlan** *interface-number* command to delete the SVI and then run the **no vlan** *vlan-id* command to delete the VLAN.

- To configure an IPv4 address, see *Configuring IPv4 Basics*.
- To configure an IPv6 address, see *Configuring IPv6 Basics*.

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 *interface-number*

No SVI is configured for a VLAN by default.

(4) (Optional) Configure an IP address for an SVI.

ip address { *ipv4-address mask* | *ipv4-address/mask-length* }

No IPv4 address is configured for an SVI by default.

1.5 Configuring Access Ports

1.5.1 Overview

Configure a Layer 2 interface as an 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 add an access port to a VLAN, the command takes effect only on access ports. If you add the access port to an inexistent VLAN, the VLAN is automatically created. Run the **no switchport access vlan** command to restore the VLAN for the access port to VLAN 1.
- In the VLAN configuration mode, run the **add interface** { *interface-type interface-number* | **range** *interface-type interface-range* } command to add an access port to the current VLAN. The command takes effect only on access ports and has the same effect as that of the **switchport access vlan** *vlan-id* command. 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.

1.5.3 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.

- Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the Layer 2 interface as an access port.

switchport mode access

The Layer 2 interface mode is **access** by default.

The Layer 2 interface mode is **hybrid** by default.

(5) Add an access port to a specified VLAN. The VLAN can be automatically created.

switchport access vlan *vlan-id*

An access port belongs to VLAN 1 by default.

An access port belongs to no VLAN by default.

1.5.4 Procedure (VLAN Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the Layer 2 interface as an access port.

switchport mode access

The Layer 2 interface mode is **access** by default.

The Layer 2 interface mode is **hybrid** by default.

(5) Return to the global configuration mode.

exit

(6) Create a VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

Only VLAN 1 exists by default.

(7) Add an access port to a VLAN. The VLAN can be automatically created. Select a method to configure the interface or the group of interfaces.

- Add a Layer 2 Ethernet interface to a VLAN.

  add interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

  An access port belongs to VLAN 1 by default.

  An access port belongs to no VLAN by default.

- Add a Layer 2 link aggregation to a VLAN.

  add interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

  An access port belongs to VLAN 1 by default.

  An access port belongs to no VLAN by default.

1.6 Configuring Trunk Ports

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 Layer 2 Ethernet interface or link aggregation as a trunk port. For more information about link aggregation, see *Configuring Aggregated Port*.

A trunk port can belong to 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. A priority packet is a tagged packet, but its VLAN ID is 0 and contains only priority information. 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.
- 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.
- Run the **no switchport mode** command to restore the Layer 2 interface mode to the default configuration.

  Run the **no switchport trunk native vlan** command to restore the native VLAN of the trunk port to a default value.

  Run the **no switchport trunk allowed vlan** command to restore the allowed VLANs of the trunk port to default values.

1.6.3 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) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the L2 interface as a trunk port.

switchport mode trunk

The Layer 2 interface mode is **access** by default.

The Layer 2 interface mode is **hybrid** by default.

(4) (Optional) Configure a native VLAN for the trunk port.

switchport trunk native vlan *vlan-id*

The native VLAN of a trunk port is VLAN 1 by default.

No native VLAN is configured for a trunk port by default.

(5) (Optional) Configure an allowed VLAN list for the trunk port.

switchport trunk allowed vlan { **all** | **add** *vlan-list* | **remove** *vlan-list* | **except** *vlan-list* | **only** *vlan-list* }

The allowed VLAN of a trunk port is VLAN 1 by default.

The allowed VLANs of a trunk port are VLANs 1 to 4094 by default.

No allowed VLAN is configured for a trunk port by default.

1.7 Configuring Uplink Ports

1.7.1 Overview

You can configure an interface as an uplink port to transmit only tagged frames of multiple VLANs. An uplink port can belong to 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.
- Run the **no switchport mode** command to restore the Layer 2 interface mode to the default configuration.

  Run the **no switchport trunk native vlan** command to restore the native VLAN of the uplink port to a

default value.

Run the **no switchport trunk allowed vlan** command to restore the allowed VLANs of the uplink port to default values.

- Run the **show vlan** [**id** *vlan-id*] and **show interface switchport** commands to check whether the configurations take effect.

1.7.3 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) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the Layer 2 interface as an uplink port.

switchport mode uplink

The Layer 2 interface mode is **access** by default.

The Layer 2 interface mode is **hybrid** by default.

(4) (Optional) Configure a native VLAN for the uplink port.

switchport trunk native vlan *vlan-id*

The native VLAN of an uplink port is VLAN 1 by default.

No native VLAN is configured for an uplink port by default.

(5) (Optional) Configure an allowed VLAN list for the uplink port.

switchport trunk allowed vlan { **all** | **add** *vlan-list* | **remove** *vlan-list* | **except** *vlan-list* | **only** *vlan-list* }

The allowed VLANs of the uplink port are VLANs 1 to 4,094 by default.

No allowed VLAN is configured for an uplink port by default.

1.8 Configuring Hybrid Ports

1.8.1 Overview

You can configure an interface as a hybrid port to transmit traffic of multiple VLANs. A hybrid port can belong to one native VLAN and several allowed VLANs.

- Native VLAN: 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: 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 a hybrid port, create these VLANs first.
- Run the **no switchport mode** command to restore the Layer 2 interface mode to the default configuration.

  Run the **no switchport hybrid native vlan** command to restore the native VLAN of the hybrid port to a default value.

  Run the **no switchport hybrid allowed vlan** command to restore the allowed VLANs of the hybrid port to default values.
- Run the **show vlan** [**id** *vlan-id*] and **show interface switchport** commands to check whether the configurations take effect.

1.8.3 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) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the Layer 2 interface as a hybrid port.

switchport mode hybrid

The Layer 2 interface mode is **access** by default.

The Layer 2 interface mode is **hybrid** by default.

(4) 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.

No native VLAN is configured for a hybrid port by default.

(5) Configure an allowed VLAN list for the hybrid port.

switchport hybrid allowed vlan { [**add**] **tagged** *vlan-list* | [**add**] **untagged** *vlan-list* | **only tagged** *vlan-list* | **remove** *vlan-list* }

By default, the allowed VLANs of a hybrid port are untagged VLAN 1 and tagged VLANs 2 to 4,094.

By default, no allowed VLAN is configured for a hybrid port.

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 Layer 2 interfaces.
debug bridge vlan	Enables the debug function of a VLAN.
show vlan id *vlan-id* **statistics**	Displays VLAN traffic statistics.
clear vlan statistics *vlan-id*	Clears the traffic statistics of a specified VLAN.

1.10 Configuration Examples

1.10.1 Configuring Layer 2 Isolation and Layer 3 Interconnection of VLANs

1. Requirements

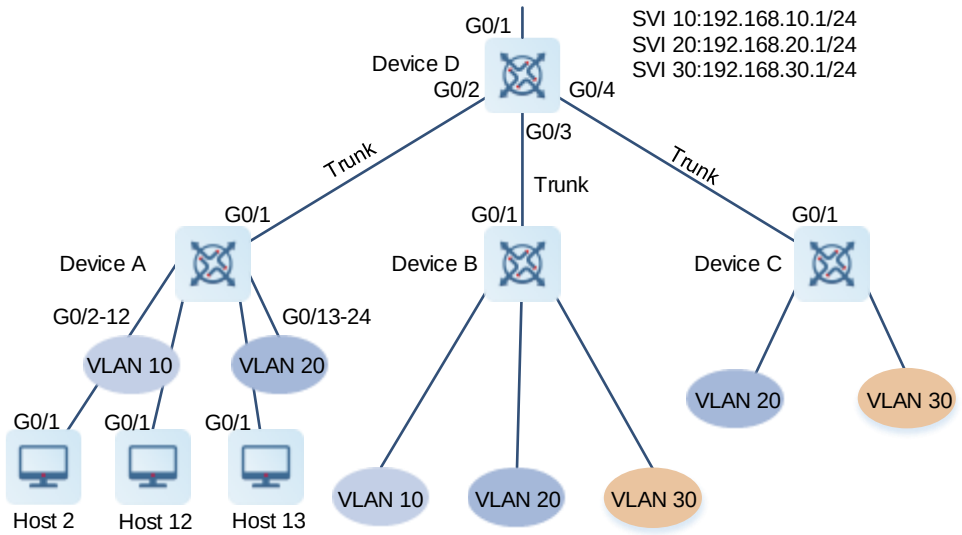
There are three departments in a user's intranet. The networks of the three departments are required to be isolated in Layer 2 and interconnected in Layer 3.

Therefore, create VLANs on the three access devices, Devices A, B, and C. The user intranet is divided into VLAN 10, VLAN 20, and VLAN 30, and they are isolated in Layer 2. Add a port to a VLAN, and all clients connected to this port belong to the VLAN. To change the VLAN of a client, modify the VLAN configuration of the port instead of moving the client.

Configure three VLANs on the core device, Device D. Configure the ports connected to Devices A, B, and C as trunk ports, and specify the allowed VLAN lists. Configure three SVIs as the gateway interfaces of the subnets of the three VLANs. The three subnets corresponding to the VLANs are 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24 respectively. The subnets of the three VLANs are interconnected through IP forwarding of Layer 3 core devices.

2. Topology

Figure 1-16 Topology of Configuring Typical Scenarios



3. Notes

- On the Layer 3 core device Device D, configure the three VLANs, configure the ports for connecting Devices A, B, and C as trunk ports, and specify an allowed VLAN list to realize Layer 2 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 respectively on the three access devices, Devices A, B, and C, assign an access port for each VLAN, and configure the port for connecting Device D as a trunk port.

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 a VLAN on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20
DeviceA(config-vlan-range)# exit
```

Create a VLAN on Devices B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 10,20,30
DeviceB(config-vlan-range)# exit
```

Create a VLAN on Devices C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# vlan range 20,30
DeviceC(config-vlan-range)# exit
```

(2) Configure IP addresses for the Layer 3 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)# exit
DeviceD(config)# interface vlan 20
DeviceD(config-if-VLAN 20)# ip address 192.168.20.1 255.255.255.0
DeviceD(config-if-VLAN 20)# exit
DeviceD(config)# 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 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 native vlan 1
DeviceD(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan only 10,20
DeviceD(config-if-GigabitEthernet 0/2)# exit
```

```
DeviceD(config)# interface gigabitethernet 0/3
DeviceD(config-if-GigabitEthernet 0/3)# switchport trunk native vlan 1
DeviceD(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan only
10,20,30
DeviceD(config-if-GigabitEthernet 0/3)# exit
DeviceD(config)# interface gigabitethernet 0/4
DeviceD(config-if-GigabitEthernet 0/4)# switchport trunk native vlan 1
DeviceD(config-if-GigabitEthernet 0/4)# switchport trunk allowed vlan only 20,30
DeviceD(config-if-GigabitEthernet 0/4)# end
DeviceD# write
```

(4) Configure the uplink port of the access device as a trunk port configure an allowed VLAN list for the port. The following example configures the uplink port on Device A. The configuration on Devices B and C is similar to that on Device A.

Configure the uplink port of Device A as a trunk port and allow the traffic of all VLANs to pass through the port.

```
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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(5) Configure the downlink port of the access device as an access port and add the port to a specified VLAN. The following example configures the downlink port on Device A. The configuration on Devices B and C is similar to that on Device A.

Configure the downlink port of Device A as an access port and add the port to different VLANs.

```
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 switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
------------------------------ ---------- --------- ------ ------ --------- --
GigabitEthernet 0/2            enabled    TRUNK     1      Disabled  10,20
GigabitEthernet 0/3            enabled    TRUNK     1      Disabled  10,20,30
GigabitEthernet 0/4            enabled    TRUNK     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 interface 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 interface 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 interface 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
switchport mode trunk
switchport trunk native vlan 1
 switchport trunk allowed vlan only 10,20
!
```

```
interface GigabitEthernet 0/3
switchport
switchport mode trunk
switchport trunk native vlan 1
 switchport trunk allowed vlan only 10,20,30
!
interface GigabitEthernet 0/4
switchport
switchport mode trunk
switchport trunk native vlan 1
 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 interfaces 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
switchport mode access
switchport access vlan 10
…
interface GigabitEthernet 0/12
switchport
switchport mode access
switchport access vlan 10
!
interface GigabitEthernet 0/13
switchport
switchport mode access
switchport access vlan 20
…
interface GigabitEthernet 0/24
switchport
switchport mode access
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.
- The trunk port of the local device sends untagged packets of the native VLAN. If the trunk port of a device produced by another manufacture only receive tagged packets, the untagged packets sent by the local device may be discarded on the receiving end. In this case, on the local device, configure the port connected to the device of another manufacture as an uplink port so that packets sent by this port are tagged.

Contents

1 Configuring MAC VLAN 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 MAC VLAN Rule 2
1.1.5 Protocols and Standards 3
1.2 Configuring MAC VLAN 3
1.2.1 Overview 3
1.2.2 Restrictions and Guidelines 3
1.2.3 Procedure 4
1.3 Monitoring 5
1.4 Configuration Examples 6
1.4.1 Configuring MAC VLAN 6

1 Configuring MAC VLAN

1.1 Introduction

1.1.1 Overview

The media access control (MAC) virtual local area network (VLAN) is a VLAN assignment technology based on MAC addresses. When the physical location of an STA changes and causes a change in the access port of the STA, MAC VLAN can assign the STA to a specified VLAN based on the MAC address of the STA, freeing you to reconfigure a VLAN for the STA's current access port.

1.1.2 Background and Function

1. Background

As mobile office is popularized, an STA connects to a network through different ports. It may connect to a network through port 1 at a time and then connect to the network through port 2 at another time. If VLANs are assigned based on ports and port 1 and port 2 belong to different VLANs, when the STA connects to the network in the second time through port 2, it is assigned to a different VLAN. In this case, the STA cannot use the resources in the VLAN to which port 1 belongs. If port 1 and port 2 belong to the same VLAN, when a second STA is connected through port 2, security issues may arise. To enable hosts of different VLANs to connect to a network through the same port, the MAC VLAN function is developed.

2. Function

The MAC VLAN function is to assign STAs to VLANs based on MAC addresses of the STAs. MAC VLAN is a VLAN assignment method based on users' MAC addresses.

This function is generally used in combination with the VLAN delivery function of IEEE 802.1X. After you configure or deliver MAC VLAN entries for a Layer 2 switch, VLANs can be assigned based on MAC addresses of STAs, thereby ensuring secure and flexible access of IEEE 802.1X-compliant STAs.

1.1.3 Principles

The MAC VLAN function must be configured on hybrid ports, and a MAC VLAN rule takes effect on all hybrid ports, on which the MAC VLAN function is enabled.

- The MAC VLAN function is available to untagged packets only. When a hybrid port receives an untagged packet, the port tries to match the source MAC address in the packet with the specified MAC address in the MAC VLAN rule.
  a. A MAC VLAN rule has a higher priority than the voice VLAN, subnet-based VLAN, protocol-based VLAN, and port VLAN rules. If the MAC VLAN function is enabled, when receiving an untagged packet, the port matches the source MAC address in the packet with the specified MAC address in the MAC VLAN rule to check whether the packet complies with the MAC VLAN rule.
  - If they match, the port changes the VLAN in the packet to the specified VLAN in the MAC VLAN rule. Then, the subsequent processing of the packet is based on this specified VLAN. For example, after an untagged packet matches a MAC VLAN rule, the VLAN learned based on the MAC address is the one redirected according to the MAC VLAN rule.

b. If they do not match, the port will match the packet against VLAN assignment rule based on packet content. The rule involves the voice VLAN, subnet-based VLAN and protocol-based VLAN. If the untagged packet matches both the MAC VLAN rule and packet content-based VLAN assignment rules, the packet is redirected to the VLAN specified in the MAC VLAN rule.

- If the port fails to match the packet with any packet content-based VLAN assignment rule, the port, according to the assignment rule of the port VLAN (common VLAN), considers that the packet belongs to the native VLAN of this port, receives the packet, and marks the packet with the native VLAN tag.

- The MAC VLAN function is unavailable to tagged packets.
- When a port receives a tagged packet, the port follows the frame receiving rules for common VLANs, and receives the packet if the port allows the packet to pass. Otherwise, the port discards the packet.
- The MAC VLAN function is unavailable to priority packets, either. In a priority packet, the VLAN ID in the VLAN tag is 0, indicating that the packet does not carry VLAN information and carries only a Class of Service (CoS) priority.

1.1.4 MAC VLAN Rule

- Configure a static MAC VLAN rule by running commands on the command line interface (CLI).

  A MAC VLAN rule reflects the mapping between a MAC address and a VLAN.

  You can configure a mapping between a MAC address and a VLAN on the CLI on a local device. Run the **show mac-vlan** command to display a MAC VLAN rule. The rule marked with "S" (static) indicates a static MAC VLAN rule.

- Configure a dynamic MAC VLAN rule by using an authentication server.

  The VLAN delivery function of IEEE 802.1X can automatically configure and deliver a mapping between a MAC address and a VLAN. Run the **show mac-vlan** command. The rule marked with "D" (dynamic) indicates a dynamic MAC VLAN rule.

  After an STA passes IEEE 802.1X authentication, the device creates a dynamic mapping between the STA's MAC address and a VLAN based on the information provided by the authentication server. After the STA goes offline, the device automatically deletes the mapping immediately.

  To use this method, configure mappings between MAC addresses and VLANs. For more information about the VLAN delivery function of IEEE 802.1X, see *Configuring IEEE 802.1X*.

- You can configure MAC VLAN rules on the local device and authentication server. If the MAC VLAN rules are consistent, they take effect concurrently. If they are inconsistent, the rule configured earlier takes effect and the rule configured later can be displayed but does not take effect. To facilitate management, you are advised to adopt one configuration method.

⚠ Caution

- If the fail VLAN function is configured in the IEEE 802.1X function, when a user fails to pass the authentication, the user packet is assigned to the fail VLAN, for example, VLAN 100. However, the static MAC VLAN rule (VLAN 200) has a higher priority. Therefore, the user packet is redirected to VLAN 200. As a result, the user cannot make communication in the fail VLAN 100. To use the fail VLAN function of the IEEE 802.1X function, do not configure a static MAC VLAN rule on the device.

1.1.5 Protocols and Standards

IEEE 802.1Q: IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 Configuring MAC VLAN

1.2.1 Overview

You can configure a static MAC VLAN entry, create a mapping between a MAC address and a VLAN, and then configure a MAC VLAN on a port so that the MAC VLAN entry takes effect on the port.

1.2.2 Restrictions and Guidelines

- The MAC VLAN function takes effect on a hybrid port only. Only an L2 interface can be configured as a hybrid port.
  - You can run the **show interface switchport** command to display the interface type. If the **Switchport** field corresponding to the interface is **enabled**, this interface is an L2 interface. If the **Switchport** field corresponding to the interface is **disabled**, this interface is an L3 interface.
  - You can run the **switchport** command to configure the interface as an L2 interface. Run the **no switchport mode** command to restore the L2 interface mode to the default mode and run the **no switchport** command to configure an L2 interface as an L3 interface. When you configure an interface as an L2 or L3 interface, all attributes of the interface are restored to the default values in this interface mode.
- Run the **mac-vlan** command to configure static MAC VLAN entries, run the **no** *mac*-**vlan** to delete static MAC VLAN entries.
- **mac-***address mac-address* indicates a MAC address. The MAC address specified in a MAC VLAN entry must be a unicast address.
- **mask** *mac-mask* indicates the mask of a MAC address. When a port with the MAC VLAN function enabled receives a packet and the packet matches a MAC VLAN entry whose mask is all F and a MAC VLAN entry whose mask is not all F, the port forwards the packet based on the latter one (indicating a larger range of MAC addresses).
  - Run the **no mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] command to delete static MAC VLAN entries of a specified MAC address.
- **vlan** *vlan-id* indicates the VLAN, to which a packet is forwarded if the MAC address in the packet matches the MAC VLAN rule. Before you configure a static MAC VLAN entry or a dynamic MAC VLAN entry is generated, make sure that the specified VLAN already exists. The specified VLAN in a MAC VLAN entry cannot be a super VLAN, a remote VLAN, or a primary VLAN. However, it can be a sub VLAN or a secondary VLAN. If an untagged packet matches both a MAC VLAN rule and a voice VLAN rule, the packet is redirected to the VLAN in the MAC VLAN rule. Run the **no mac-vlan vlan** *vlan-id* command to delete the static MAC VLAN entries of a specified VLAN.
- **priority** *priority-value* indicates the 802.1p priority. The default value is **0**. When a packet matches a MAC VLAN rule, the receiving port of the packet changes the CoS priority of the packet to the value of *priority-value*. If the packet priority needs to be modified, ensure that the Quality of Service (QoS) module trusts the packet priority modified by an interface. Otherwise, the modification is invalid. If an untagged packet matches both a MAC VLAN rule and a voice VLAN rule, the packet priority is modified according to

the voice VLAN rule.

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 MAC VLAN function. Run the **mls qos trust** { **cos** | **ip-precedence** | **dscp** | **exp** } command in interface configuration mode, and select the **cos** parameter to enable the QoS module to trust the CoS modification, that is, the packet priority modified by the MAC VLAN function.

- Run the **no mac-vlan all** command to delete all MAC VLAN entries.
- Run the **mac-vlan enable** command to enable the MAC VLAN function on ports so that the function can take effect. Otherwise, the MAC VLAN function does not take effect even if there are global MAC VLAN entries.
- You must complete interface configuration before you enable the MAC VLAN function on a port. Otherwise, the allowed VLAN list of the port cannot be modified.

1.2.3 Procedure

(1) Create a MAC VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a MAC VLAN.

vlan { *vlan-id* | **range** *vlan-range* }

By default, no VLAN other than VLAN 1 exists.

d Exit the VLAN configuration mode.

exit

(2) Configure a static MAC VLAN rule in global configuration mode, and specify a mapping between a MAC address and a VLAN in the rule.

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *priority-value*]

No static MAC VLAN rule exists by default.

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the Layer 2 interface as a hybrid port.

switchport mode hybrid

The default Layer 2 interface mode is the access mode.

(5) Add the MAC VLAN to the allowed untagged VLAN list of the hybrid port.

switchport hybrid allowed vlan untagged *vlan_list*

The allowed untagged VLAN of the hybrid port is VLAN 1 by default.

(6) Configure the hybrid port to trust the CoS priority of packets.

mls qos trust cos

The default trust mode of a port is untrusted.

(7) Enable the MAC VLAN function on the port.

mac-vlan enable

The port-based MAC VLAN function is disabled 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.

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 1-1 Monitoring

Command	Purpose
show mac-vlan all	Displays all MAC VLAN entries, including static and dynamic MAC VLAN entries.
show mac-vlan dynamic	Displays dynamic MAC VLAN entries.
show mac-vlan static	Displays static MAC VLAN entries.
show mac-vlan vlan vlan-id	Displays MAC VLAN entries of a specified VLAN.
show mac-vlan interface	Displays ports on which the MAC VLAN function is enabled.
show mac-vlan mac-address *mac-address* [**mask** *mac-mask*]	Displays MAC VLAN entries of a specified MAC address.
debug bridge mvlan	Debugs the MAC VLAN function.

1.4 Configuration Examples

1.4.1 Configuring MAC VLAN

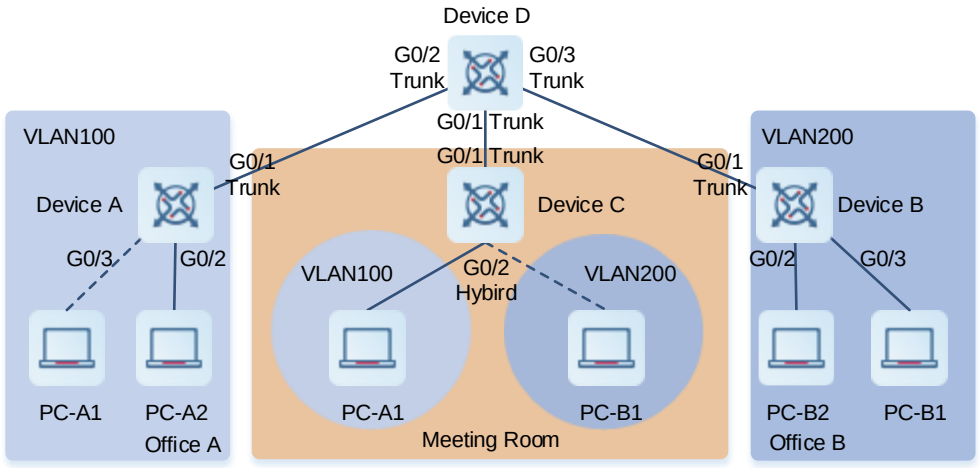
1. Requirements

A company provide a temporary office in a meeting room where public access ports are assigned to VLANs based on the MAC addresses of employees' portable PCs. Employee PCs connected to any port are automatically assigned to their respective department VLANs.

2. Topology

PC-A1 and PC-A2 belong to department A and they are assigned to VLAN 100. PC-B1 and PC-B2 belong to department B and they are assigned to VLAN 200. The meeting room uses public ports. PC-A1 and PC-A2 can be assigned only to VLAN 100 after access and PC-B1 and PC-B2 can be assigned only to VLAN 200.

Figure 1-1 Topology of Configuring MAC VLAN



3. Notes

- On Device D, configure the ports connecting to access devices as trunk ports.
- Create MAC VLANs on Device C and configure static MAC VLAN rules in global configuration mode.
  - Department A uses a PC with the MAC address of 54bf.6450.dd10 for access in the meeting room, and the PC is assigned to VLAN 100 with a priority of 1.
  - Department B uses multiple PCs for access in the meeting room. Their MAC addresses are in the range from 54bf.6450.dd20 to 54bf.6450.dd2F (represented with 54bf.6440.dd20 plus the mask of ffff.ffff.fff0). The PCs are assigned to VLAN 200 with a priority of 2.
- On Device C, configure the ports connecting to PCs as hybrid ports, and add the MAC VLANs to the allowed untagged VLAN list of the ports. Configure the ports to trust the CoS priority of packets. Enable the MAC VLAN function on the ports.
- Configure the uplink ports on Device A and Device B as trunk ports, and the ports connecting to PCs as access ports. Add the access ports on Device A to VLAN 100, and add the access ports on Device B to VLAN 200.

4. Procedure

(1) Create VLANs.

Configure VLAN 100 and VLAN 200 on Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# vlan range 100,200
DeviceD(config-vlan-range)# exit
```

Configure VLAN 100 and VLAN 200 on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# vlan rang 100,200
DeviceC(config-vlan-range)# exit
```

Configure VLAN 100 on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 100
DeviceA(config-vlan-range)# exit
```

Configure VLAN 200 on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 200
DeviceB(config-vlan-range)# exit
```

(2) Configure trunk ports.

Configure the downlink ports GigabitEthernet 0/1–3 of Device D as trunk ports.

```
DeviceD(config)# interface range gigabitethernet 0/1-3
DeviceD(config-if-range)# switchport
DeviceD(config-if-range)# switchport mode trunk
DeviceD(config-if-range)# switchport trunk native vlan 1
DeviceD(config-if-range)# switchport trunk allowed vlan all
DeviceD(config-if-range)# end
DeviceD# write
```

Configure the uplink ports GigabitEthernet 0/1 of Devices A/B/C as trunk ports. The configurations on Devices A, B, and C are similar. The following examples takes Device A as an example.

```
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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(3) Add user ports to static VLANs on Devices A and B.

Add the user ports GigabitEthernet 0/2–3 on Device A to VLAN 100.

```
DeviceA(config)# interface range gigabitethernet 0/2-3
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode access
DeviceA(config-if-range)# switchport access vlan 100
DeviceA(config-if-range)# end
DeviceA# write
```

Add the user ports GigabitEthernet 0/2–3 on Device B to VLAN 200.

```
DeviceB(config)# interface range gigabitethernet 0/2-3
DeviceB(config-if-range)# switchport
DeviceB(config-if-range)# switchport mode access
DeviceB(config-if-range)# switchport access vlan 200
DeviceB(config-if-range)# end
DeviceB# write
```

(4) Add the user port GigabitEthernet 0/2 on Device C to VLANs based on the MAC addresses of PCs.

Create a static MAC VLAN rule in global configuration mode.

```
DeviceC(config)# mac-vlan mac-address 54bf.6450.dd10 vlan 100 priority 1
DeviceC(config)# mac-vlan mac-address 54bf.6450.dd20 mask ffff.ffff.fff0 vlan 200
priority 2
```

Configure the downlink port GigabitEthernet 0/2 as a hybrid port, and add the MAC VLANs to the allowed untagged VLAN list of the port.

```
DeviceC(config)# interface gigabitethernet 0/2
DeviceC(config-if-GigabitEthernet 0/2)# switchport
DeviceC(config-if-GigabitEthernet 0/2)# switchport mode hybrid
DeviceC(config-if-GigabitEthernet 0/2)# switchport hybrid native vlan 1
DeviceC(config-if-GigabitEthernet 0/2)# switchport hybrid allowed vlan add
untagged 1,100,200
```

Configure the port to trust the CoS priority of packets.

```
DeviceC(config-if-GigabitEthernet 0/2)# mls qos trust cos
```

Enable the MAC VLAN function on the port.

```
DeviceC(config-if-GigabitEthernet 0/2)# mac-vlan enable
DeviceC(config-if-GigabitEthernet 0/2)# end
DeviceC# write
```

5. Verification

(1) Run the **show mac-vlan interface** command to display ports on which the MAC VLAN function is enabled.

```
DeviceC# show mac-vlan interface
MAC VLAN is enabled on following interface:
---------------------------------------
GigabitEthernet 0/2
```

(2) Run the **show interface** command to verify that packets sent by port GigabitEthernet 0/2 to the MAC VLAN do not carry tags.

```
DeviceC(config-if-GigabitEthernet 0/2)# show interface gigabitethernet 0/2
  Bridge attributes:
```

```
   Port-type: hybrid
Tagged vlan id: 2-99,101-199,201-4094
Tagged vlan id: None
Untagged vlan id: 1,100,200
```

(3) Check static MAC VLAN entries on Device C.

```
DeviceC# show mac-vlan static
The following MAC VLAN address exist:
S: Static   D: Dynamic
MAC ADDR          MASK           VLAN ID   PRIO   STATE
-------------------------------------------------------
54bf.6450.dd10     ffff.ffff.ffff   100      1      S
54bf.6450.dd20     ffff.ffff.fff0   200      2      S
Total MAC VLAN address count: 2
```

(4) To verify that the MAC VLAN function assigns STAs to different VLANs to implement L2 isolation, assign PC-A1, PC-A2, and PC-B2 to the same network segment and ping the STAs. Only STAs in the same VLAN can be pinged successfully.

Connect PC-A2 to the network through office A, assign PC-A2 to VLAN 100, and set its IP address and mask to 192.168.5.12/24.

```
PC-A2> enable
PC-A2# configure terminal
PC-A2(config)# interface gigabitethernet 0/1
PC-A2(config-if-GigabitEthernet 0/1)# no switchport
PC-A2(config-if-GigabitEthernet 0/1)# ip address 192.168.5.12/24
```

Connect PC-B2 to the network through office B, assign PC-B2 to VLAN 200, and set its IP address and mask to 192.168.5.22/24.

```
PC-B2> enable
PC-B2# configure terminal
PC-B2(config)# interface gigabitethernet 0/1
PC-B2(config-if-GigabitEthernet 0/1)# no switchport
PC-B2(config-if-GigabitEthernet 0/1)# ip address 192.168.5.22/24
```

Connect PC-A1 to the network through the meeting room and set its IP address and mask to 192.168.5.11/24. Verify that PC-A1 can ping PC-A2 in VLAN 100 but cannot ping PC-B2 in VLAN 200. This indicates that PC-A1 is assigned to VLAN 100 by the MAC VLAN function.

```
PC-A1> enable
PC-A1# configure terminal
PC-A1(config)# interface gigabitethernet 0/1
PC-A1(config-if-GigabitEthernet 0/1)# no switchport
PC-A1(config-if-GigabitEthernet 0/1)# ip address 192.168.5.11/24
PC-A1(config-if-GigabitEthernet 0/1)# end
PC-A1# ping 192.168.5.12
Sending 5, 100-byte ICMP Echoes to 192.168.5.12, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/22/103 ms.
```

```
PC-A1# ping 192.168.5.22
Sending 5, 100-byte ICMP Echoes to 192.168.5.22, timeout is 2 seconds:
  < press Ctrl+C to break >
....
Success rate is 0 percent (0/5).
```

6. Configuration Files

- Device C configuration file

```
vlan range 1,100,200
!
mac-vlan mac-address 54bf.645c.dd10 vlan 100 priority 1
mac-vlan mac-address 54bf.6450.dd20 mask ffff.ffff.fff0 vlan 200 priority 2
!
interface GigabitEthernet 0/1
switchport
 switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
 switchport mode hybrid
switchport hybrid native vlan 1
switchport hybrid allowed vlan only tagged 2-99,101-199,201-4094
switchport hybrid allowed vlan add untagged 1,100,200
mls qos trust cos
mac-vlan enable
```

- Device A configuration file

```
vlan range 1,100
!
interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
switchport mode access
switchport access vlan 100
!
interface GigabitEthernet 0/3
switchport
switchport mode access
switchport access vlan 100
```

- Device B configuration file

```
vlan range 1,200
!
interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- Device D configuration file

```
vlan range 1,100,200
!
interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

7. Common Errors

- An Ethernet interface or aggregated port is not configured as a Layer 2 interface before the MAC VLAN function is configured on the interface.
- The QoS module does not trust the packet priority modified by an interface. As a result, the MAC VLAN priority configuration does not take effect.

Contents

1 Configuring Protocol-based VLAN 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Subnet-based VLAN 1
1.1.3 Protocol-based VLAN 1
1.1.4 Principles 1
1.1.5 Protocols and Standards 2
1.2 Restrictions and Guidelines 2
1.3 Configuration Task Summary 2
1.4 Configuring the Subnet-based VLAN Function 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 3
1.4.3 Prerequisites 3
1.4.4 Procedure 3
1.5 Configuring the Protocol-based VLAN Function 4
1.5.1 Overview 4
1.5.2 Restrictions and Guidelines 4
1.5.3 Prerequisites 5
1.5.4 Procedure 5
1.6 Monitoring 6
1.7 Configuration Examples 7
1.7.1 Configuring Subnet-based VLANs 7

1.7.2 Configuring Protocol-based VLANs 11

1 Configuring Protocol-based VLAN

1.1 Introduction

1.1.1 Overview

Protocol-based VLAN is a VLAN technology based on protocol types. When a device receives a packet without a VLAN ID from a port, the device automatically forwards the packet to a VLAN specified in a user-defined rule if the packet matches the user-defined rule.

The protocol VLAN is divided into subnet-based VLAN and protocol-based VLAN.

1.1.2 Subnet-based VLAN

VLAN assignment based on source IP address and subnet mask in a packet is referred to as subnet-based VLAN.

The subnet-based VLAN function assigns users to different VLANs based on their IP addresses. For example, in a shared office area, IP addresses of users are fixed, but the access ports are dynamic. To control user access to network resources, you can assign users to different VLANs based on their IP addresses.

⚠ Caution

Subnet-based VLANs take effect on trunk and hybrid ports, available to packets without VLAN ID only.

1.1.3 Protocol-based VLAN

VLAN assignment based on packet type and Ethernet type is referred to as protocol-based VLAN.

The protocol-based VLAN function is used to assign packets of different service types to different VLANs to facilitate management and maintenance.

⚠ Caution

Protocol-based VLANs take effect on trunk and hybrid ports. This function is available to packets without VLAN ID only.

1.1.4 Principles

When a port receives a packet, the port assigns the packet to a VLAN so that the packet belongs to this VLAN only. The procedure of determining a VLAN for a packet is as follows:

(1) If the packet carries a tag and the tag contains a VLAN ID, the packet belongs to the VLAN specified by the VLAN ID. The port receives the packet if the port allows the packet to pass. Otherwise, the port discards the packet.

(2) If the packet does not carry a VLAN ID (untagged packet or a priority packet with the VLAN ID of 0), the port tries to match the packet with VLAN assignment policies based on priority in descending order. If the packet matches a rule, the packet is assigned to the VLAN specified in the rule. If the packet matches multiple rules at the same time, the packet is forwarded based on the rule with the highest priority.

a A MAC VLAN policy has the highest priority. A packet with the MAC address matching a MAC VLAN rule is assigned to the MAC VLAN specified in the rule. The MAC VLAN policy is unavailable to priority packets.

b If a voice VLAN policy exists, a device identifies a voice packet based on the MAC address or voice organizationally unique identification (OUI) and then forwards the packet to the specified voice VLAN.

c If the IP address in a packet matches an IP address in a rule of a subnet-based VLAN policy, the packet is assigned to the subnet-based VLAN specified in the rule.

d If the packet type and Ethernet type of a packet match those configured in a rule of a protocol-based VLAN policy, the packet is assigned to the protocol-based VLAN specified in the rule.

(3) A packet is assigned to the port VLAN (access port) or native VLAN (trunk/hybrid/uplink port) in any one of the following cases: The policy-based VLAN assignment function is disabled, no policy exists, or the packet does not match any policy.

1.1.5 Protocols and Standards

- IEEE 802.1Q: IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 Restrictions and Guidelines

- The subnet-based VLAN and protocol-based VLAN function only take effect on a Layer 2 interface and the L2 interface must be a trunk or hybrid port.
- You can run the **show interface switchport** command to display the interface type. If the **Switchport** field corresponding to the interface is enabled, this interface is a Layer 2 interface. If the **Switchport** field corresponding to the interface is disabled, this interface is a Layer 3 interface.
- You can run the **switchport** command to configure the interface as a Layer 2 interface. Run the **no switchport mode** command to restore the L2 interface mode to the default mode and run the **no switchport** command to configure a Layer 2 interface as an L3 interface. When you configure an interface as a Layer 2 or Layer 3 interface, all attributes of the interface are restored to the default values in this interface mode.

1.3 Configuration Task Summary

Protocol-based VLAN configuration include the following optional tasks. Select the configuration tasks as required.

- Configuring the Subnet-based VLAN Function
- Configuring the Protocol-based VLAN Function

1.4 Configuring the Subnet-based VLAN Function

1.4.1 Overview

You can configure VLAN assignment based on IP addresses so that packets from a specified network segment or a specified IP address are forwarded to the specified VLAN.

1.4.2 Restrictions and Guidelines

- The subnet-based VLAN function takes effect on trunk or hybrid ports only. You must configure a port as a trunk or hybrid port and then run the **protocol-vlan ipv4** command to configure the subnet-based VLAN function.
- To enable the subnet-based VLAN function on a trunk or hybrid port, add all subnet-based VLANs to the allowed VLAN list of the trunk or hybrid port.
- You can enable the subnet-based VLAN function in interface configuration mode without global subnet-based VLAN configuration. However, you must enable the subnet-based VLAN function in both the global and interface configuration mode so that the subnet-based VLAN function takes effect.

1.4.3 Prerequisites

Configure a Layer 2 interface by running the **switchport** command.

1.4.4 Procedure

(1) Configure subnet-based VLAN rules in global configuration mode.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN by configuring a policy.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

e Configure subnet-based VLAN rules one by one in global configuration mode, and assign a specified subnet to the specified VLAN.

protocol-vlan ipv4 *ip-address* **mask** *mask* **vlan** *vlan-id*

No global subnet-based VLAN rule is configured by default.

(2) Enter the interface configuration mode and configure subnet-based VLAN.

a Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

b Enter the Layer 2 link aggregation configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the port as a trunk or hybrid port.

switchport mode { **trunk | hybrid** }

The default Layer 2 interface mode is the access mode.

(4) Add subnet-based VLANs to the allowed VLAN list of an interface. Configure one of the following tasks.

o Configure an allowed VLAN list for the trunk port.

switchport trunk allowed vlan { **add** *vlan-list* | **all** | **except** *vlan-list* | **only** *vlan-list* | **remove** *vlan-list* }

The default allowed VLANs of the trunk port are VLANs 1 to 4094.

- Configure an allowed VLAN list for the hybrid port.

  switchport hybrid allowed vlan { [**add**] **tagged** *vlan-list* | [**add**] **untagged** *vlan-list* | **only tagged** *vlan-list* | **remove** *vlan-list* }

  The default allowed VLANs of the hybrid port are untagged VLAN 1 and tagged VLANs 2 to 4094.

(5) Enable the subnet-based VLAN function on the interface.

protocol-vlan ipv4

The subnet-based VLAN function is disabled by default.

1.5 Configuring the Protocol-based VLAN Function

1.5.1 Overview

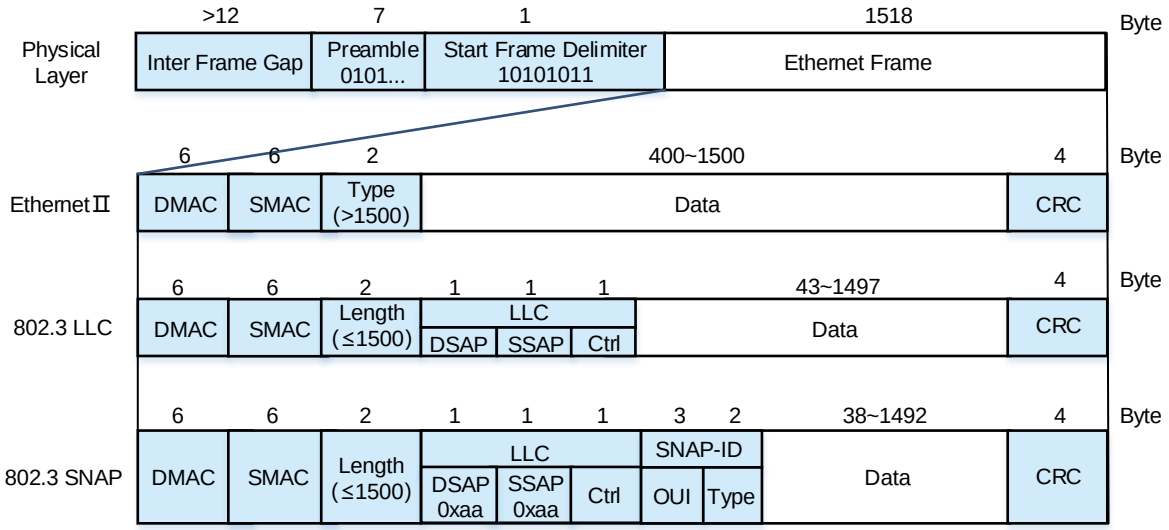
Protocol-based VLAN assigns packets of different service types to different VLANs to facilitate management and maintenance. Figure 1-1 shows the frame format.

This function uses **frame-type** to indicate a frame type, and supports the **EtherII**, **SNAP** and **LLC** frame types.

If the frame type is **EtherII** or **SNAP**, the **ether-type** *type* parameter is used to configure the Ethernet packet type.

If the frame type is **LLC**, the **dsap** *value* **ssap** *value* parameter is used to configure the type of a service access point (SAP).

Figure 1-1 Ethernet Frame Format



1.5.2 Restrictions and Guidelines

- The protocol-based VLAN function takes effect on trunk or hybrid ports only. You must configure an interface as a trunk or hybrid port and then run the **protocol-vlan profile vlan** command to configure the protocol-based VLAN function.

- To configure and enable the protocol-based VLAN function on a trunk or hybrid port, add all protocol-based VLANs to the allowed VLANs of the trunk or hybrid port.
- Configure the protocol-based VLAN packet type in global configuration mode, configure specified VLANs in the interface configuration mode, and enable the protocol-based VLAN function. Then the protocol-based VLAN function takes effect. When you delete the global configuration, the protocol-based VLAN configuration of all interfaces related to profile number is automatically deleted.
- **profile** *profile-number* specifies the number of a protocol-based VLAN rule (profile). The value range of this parameter is from 1 to 8.
- **frame-type**: Specifies a frame type. The values include **EtherII**, **SNAP**, and **LLC**. If the frame type is **EtherII** or **SNAP**, configure the **ether-type** *type* parameter to specify the corresponding Ethernet type. When the frame type is **LLC**, configure the **dsap** *value* **ssap** *value* parameter to specify the corresponding SAP type.
- **ether-type** *type* specifies an Ethernet type of frames. The value range is from 1501 to 65535 (in decimal notation of the protocol ID). The value can also be a protocol name or the protocol ID in hexadecimal notation. The supported protocols include AARP (0x80f3), AMBER (0x6008), APPLETALK (0x809b), ARP (0x0806), CFM (0x8902), DECNET-IV (0x6003), DIAGNOSTIC (0x6005), EAPOL (0x888e), FC_ETH, HEX6000 (0x6000), HEX8042 (0x8042), IPv4 (0x0800), IPv6 (0x86DD), IPX (0x8137), LAT (0x6004), LAVC-SCA (0x6007), MAC_IN_MAC (0x88E7), MOP-CONSOLE (0x6002), MOP-DUMP (0x6001), MUMPS (0x6009), NETBIOS (0x8040), SNX-IDP (0x0600), VINES-ECHO (0x0baf), and X-25 (0x0805).
- In the **dsap** *value* **ssap** *value* parameter, **dsap** specifies a destination service access point (DSAP), and **ssap** specifies a source service access point (SSAP). The range of *value* is from 0 to 255, corresponding to 0x00 to 0xFF of one byte in hexadecimal notation. For example, if an IP packet is encapsulated into a Logical Link Control (LLC) frame, the DSAP value and SSAP value are both 0x06.
- *vlan-id* specifies a VLAN ID. The value range is from 1 to 4094.

1.5.3 Prerequisites

Configure an interface as a Layer 2 interface by running the **switchport** command.

1.5.4 Procedure

(1) Create a VLAN assigned by the protocol-based VLAN policy.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN by configuring a policy.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure protocol VLAN rules one by one in global configuration mode.

protocol-vlan profile *profile-number* **frame-type** { **etherII ether-type** *type* | **snap ether-type** *type* | **llc dsap** *value* **ssap** *value* }

protocol-vlan profile *profile-number* **ether-type** *type*

No global protocol-based VLAN rule is configured by default.

(3) Enter the interface configuration mode and configure protocol-based VLAN.

a Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

b Enter the Layer 2 link aggregation configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the port as a trunk or hybrid port.

switchport mode { **trunk | hybrid** }

The default Layer 2 interface mode is the access mode.

(5) Add protocol-based VLANs to the allowed VLAN list of an interface. Configure one of the following tasks.

- Configure an allowed VLAN list for the trunk port.

  switchport trunk allowed vlan { **all** | **add** *vlan-list* | **remove** *vlan-list* | **except** *vlan-list* | **only** *vlan-list* }

  The default allowed VLANs of the trunk port are VLANs 1 to 4094.

- Configure an allowed VLAN list for the hybrid port.

  switchport hybrid allowed vlan { [**add**] **tagged** *vlan-list* | [**add**] **untagged** *vlan-list* | **only tagged** *vlan-list* | **remove** *vlan-list* }

  The default allowed VLANs of the hybrid port are untagged VLAN 1 and tagged VLANs 2 to 4094.

(6) Configure protocol-based VLAN rules one by one on the interface so that packets that match the *num* rule are assigned to the VLAN specified by VLAN *vlan-id*.

protocol-vlan profile *profile-number* **vlan** *vlan-id*

The protocol-based VLAN function 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 **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** command may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
show protocol-vlan	Displays configurations of all protocol-based VLANs.
show protocol-vlan profile	Displays the protocol-based VLAN configuration.
show protocol-vlan ipv4	Displays the subnet-based VLAN configuration.
debug bridge protvlan	Debugs the protocol-based VLAN function.

1.7 Configuration Examples

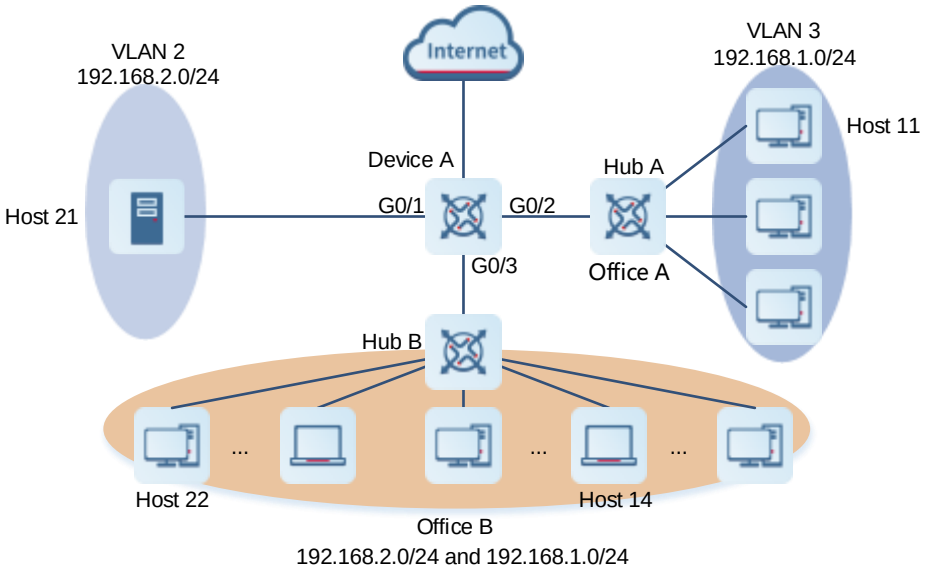
1.7.1 Configuring Subnet-based VLANs

1. Requirements

Office area A and office area B are connected to Layer 3 device A through hubs. In office area A, hosts belong to a fixed network segment and are assigned to VLANs based on ports. In shared office area B, there are two network segments of hosts. Such hosts are not connected through fixed access ports and therefore they cannot be assigned to VLANs based on ports. Device A must assign hosts in office area B to VLANs based on the IP address segments, to which user packets belong.

2. Topology

Figure 1-2 Topology of Configuring Subnet-based VLANs



3. Notes

- Configure VLAN 2 and VLAN 3 on device A.
- Configure GigabitEthernet 0/1 as an access port and assign the port to VLAN 2. Configure GigabitEthernet 0/2 as an access port and assign the port to VLAN 3.

- Configure a subnet-based VLAN rule in global configuration mode on device A and assign the IP address segment 192.168.2.0/24 to VLAN 2 and the IP address segment 192.168.1.0/24 to VLAN 3.
- Configure GigabitEthernet 0/3 as a hybrid port, add untagged VLAN 2 and VLAN 3 to the allowed VLAN list of the port, and enable the subnet-based VLAN function on GigabitEthernet 0/3.

4. Procedure

(1) Create VLANs to be assigned based on subnets. Configure a global subnet-based VLAN rule, in which packets with IP addresses in the network segment of 192.168.1.0/24 are assigned to VLAN 3 and packets with IP addresses in the network segment of 192.168.2.0/24 are assigned to VLAN 2.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 2-3
DeviceA(config-vlan)# exit
DeviceA(config)# protocol-vlan ipv4 192.168.1.0 mask 255.255.255.0 vlan 3
DeviceA(config)# protocol-vlan ipv4 192.168.2.0 mask 255.255.255.0 vlan 2
```

(2) Configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as access ports and add them to different VLANs.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 2
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 access vlan 3
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(3) Configure GigabitEthernet 0/3 that will run the subnet-based VLAN function as a hybrid port, and allow packets from the subnet-based VLANs to pass.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# switchport
DeviceA(config-if-GigabitEthernet 0/3)# switchport mode hybrid
DeviceA(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged
2-3
```

(4) Enable the subnet-based VLAN function on GigabitEthernet 0/3 that needs to run the subnet-based VLAN function.

```
DeviceA(config-if-GigabitEthernet 0/3)# protocol-vlan ipv4
```

5. Verification

(1) Run the **show protocol-vlan ipv4** command to check whether the protocol-based VLAN configuration on the device is correct.

```
DeviceA# show protocol-vlan ipv4
ip            mask          vlan
--------------- --------------- ----
192.168.1.0    255.255.255.0   3
192.168.2.0    255.255.255.0   2
interface          ipv4 status
```

```
-------------------- -----------
Gi0/3              enable
```

(2) Take hosts 21, 22, 11, and 14 as examples to verify the subnet-based VLAN assignment effect.

Set the default gateway address of host 21 in VLAN 2 to 192.168.2.1, and the IP address to 192.168.2.21/24.

```
Host21> enable
Host21# configure terminal
Host21(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1
Host21(config)# interface gigabitethernet 0/1
Host21(config-if-GigabitEthernet 0/1)# no switchport
Host21(config-if-GigabitEthernet 0/1)# ip address 192.168.2.21/24
Host21(config-if-GigabitEthernet 0/1)# end
```

Set the default gateway address of host 22 in VLAN 2 to 192.168.2.1, and the IP address to 192.168.2.22/24.

```
Host22> enable
Host22# configure terminal
Host22(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1
Host22(config)# interface gigabitethernet 0/1
Host22(config-if-GigabitEthernet 0/1)# no switchport
Host22(config-if-GigabitEthernet 0/1)# ip address 192.168.2.22/24
Host22(config-if-GigabitEthernet 0/1)# end
```

Set the default gateway address of host 11 in VLAN 3 to 192.168.1.1, and the IP address to 192.168.1.11/24.

```
Host11> enable
Host11# configure terminal
Host11(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
Host11(config)# interface gigabitethernet 0/1
Host11(config-if-GigabitEthernet 0/1)# no switchport
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.1.11/24
Host11(config-if-GigabitEthernet 0/1)# end
```

Set the default gateway address of host 14 in VLAN 3 to 192.168.1.1, and the IP address to 192.168.1.14/24.

```
Host14> enable
Host14# configure terminal
Host14(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
Host14(config)# interface gigabitethernet 0/1
Host14(config-if-GigabitEthernet 0/1)# no switchport
Host14(config-if-GigabitEthernet 0/1)# ip address 192.168.1.14/24
Host14(config-if-GigabitEthernet 0/1)# end
```

Verify that host 22 is assigned to VLAN 2 by the subnet-based VLAN function, and host 22 can ping host 21 in VLAN 2 but cannot ping host 11 in VLAN 3.

```
Host22# ping 192.168.2.21
Sending 5, 100-byte ICMP Echoes to 192.168.2.21, timeout is 2 seconds:
```

```
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms.
Host22# 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 0 percent (0/5).
```

Verify that host 14 is assigned to VLAN 3 by the subnet-based VLAN function, and host 14 can ping host 11 in VLAN 3 but cannot ping host 21 in VLAN 2.

```
Host14# 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 = 2/2/4 ms.
Host14# ping 192.168.2.21
Sending 5, 100-byte ICMP Echoes to 192.168.2.21, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

Configure the IP addresses of the SVI gateways for VLAN 2 and VLAN 3 on device A to implement L3 connection between the VLANs.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ip address 192.168.2.1/24
DeviceA(config-if-VLAN 2)# exit
DeviceA(config)# interface vlan 3
DeviceA(config-if-VLAN 3)# ip address 192.168.1.1/24
DeviceA(config-if-VLAN 2)# end
```

Verify that host 14 in VLAN 3 can ping host 21 in VLAN 2. Likewise, verify that host 22 in VLAN 3 can ping host 21 in VLAN 2.

```
Host14# ping 192.168.2.21
Sending 5, 100-byte ICMP Echoes to 192.168.2.21, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/19/79 ms.
```

6. Configuration Files

Device A configuration file

```
protocol-vlan ipv4 192.168.1.0 mask 255.255.255.0 vlan 3
protocol-vlan ipv4 192.168.2.0 mask 255.255.255.0 vlan 2
!
vlan range 2-3
```

```
!
interface GigabitEthernet 0/1
switchport
switchport mode access
switchport access vlan 2
!
interface GigabitEthernet 0/2
switchport
switchport mode access
switchport access vlan 3
!
interface GigabitEthernet 0/3
switchport
switchport mode hybrid
switchport hybrid allowed vlan only tagged 4-4094
switchport hybrid allowed vlan add untagged 1-3
protocol-vlan ipv4
```

7. Common Errors

- A port connected to the device is not a trunk or hybrid port.
- The allowed VLAN list of the port connected to the device does not contain the user communication VLANs.
- The subnet-based VLAN function is disabled on a port.
- Packets match a VLAN assignment policy with a higher priority (for example, MAC VLAN or voice VLAN) on the port, causing the failure of the subnet-based VLAN policy to take effect.

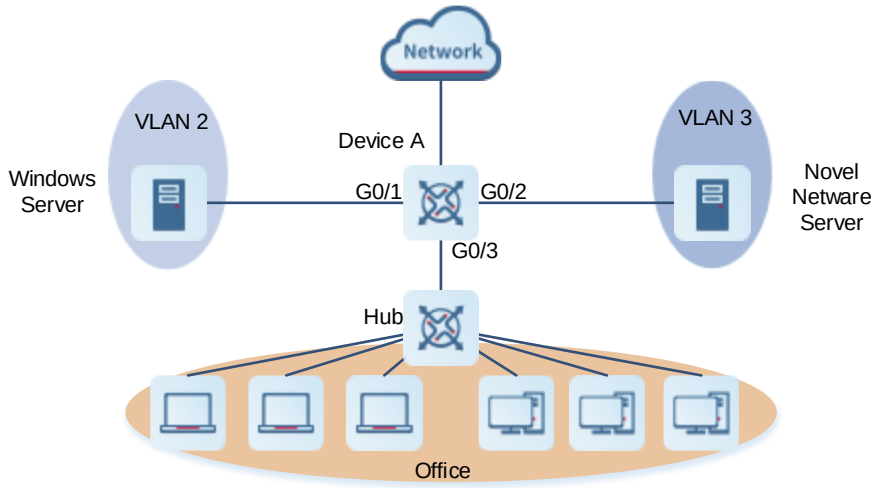
1.7.2 Configuring Protocol-based VLANs

1. Requirements

In an office area, some PCs run the Windows NT operating system (OS) and support the IP protocol, and some run the Novell Netware OS and support the Internetwork Packet Exchange (IPX) protocol. Two servers in the office network are used to isolate hosts running different OSs at L2 so that the hosts running Windows NT can access only the Windows NT server and the hosts running Novell Netware can access only the Novell Netware server. The purpose is to reduce network traffic.

2. Topology

Figure 1-3 Topology of Configuring Protocol-based VLAN



3. Notes

- Configure VLAN 2 and VLAN 3 on device A.
- Configure GigabitEthernet 0/1 as an access port and assign the port to VLAN 2. Configure GigabitEthernet 0/2 as an access port and assign the port to VLAN 3.
- Configure protocol-based VLAN rules in global configuration mode on device A so that IP packets match rule 1 and IPX packets match rule 2.
- Configure GigabitEthernet 0/3 as a hybrid port and add VLAN 2 and VLAN 3 to the allowed untagged VLAN list of the port. Enable the protocol-based VLAN function on GigabitEthernet 0/3, and associate rule 1 with VLAN 2 and rule 2 with VLAN 3.

4. Procedure

(1) Create VLAN 2 and VLAN 3 to be assigned according to protocol rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 2-3
DeviceA(config-vlan)# exit
```

(2) Configure protocol-based VLAN rules in global configuration mode.

Apply rule 1 to IP packets whose frame type is EthernetII and Ethernet type is 0x0800.

```
DeviceA(config)# protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800
```

Apply rule 2 to IPX packets whose frame type is EthernetII and Ethernet type is 0x8137.

```
DeviceA(config)# protocol-vlan profile 2 frame-type ETHERII ether-type 0x8137
```

(3) Configure ports that connect to servers as access ports and add the ports to different VLANs.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport
DeviceA(config-if-GigabitEthernet 0/1)# switchport access vlan 2
```

```
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 access vlan 3
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(4) Configure the port that needs to run the protocol-based VLAN function as a hybrid port, and add VLAN 2 and VLAN 3 to the allowed VLAN list of the port.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# switchport
DeviceA(config-if-GigabitEthernet 0/3)# switchport mode hybrid
DeviceA(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged
2-3
```

(5) Enable the protocol-based VLAN function on GigabitEthernet 0/3, and assign packets that match rule 1 to VLAN 2 and packets that match rule 2 to VLAN 3.

```
DeviceA(config-if-GigabitEthernet 0/3)# protocol-vlan profile 1 vlan 2
DeviceA(config-if-GigabitEthernet 0/3)# protocol-vlan profile 2 vlan 3
```

5. Verification

Run the **show protocol-vlan profile** [*profile-number*] command to check whether the protocol-based VLAN configuration on the device is correct.

```
DeviceA(config)# show protocol-vlan profile
profile frame-type      ether-type/DSAP+SSAP   interface      vlan
------- --------------- ---------------------- --------------- ----
1      ETHERII         0x0800               Gi0/3         2
2      ETHERII         0x8137               Gi0/3         3
```

6. Configuration Files

Device A configuration file

```
protocol-vlan profile 1 frame-type ETHERII ether-type IPV4
protocol-vlan profile 2 frame-type ETHERII ether-type IPX
!
vlan range 2-3
!
interface GigabitEthernet 0/1
switchport
switchport mode access
switchport access vlan 2
!
interface GigabitEthernet 0/2
switchport
switchport mode access
switchport access vlan 3
!
interface GigabitEthernet 0/3
switchport
```

```
switchport mode hybrid
switchport hybrid allowed vlan only tagged 4-4094
switchport hybrid allowed vlan add untagged 1-3
protocol-vlan profile 1 vlan 2
protocol-vlan profile 2 vlan 3
```

7. Common Errors

- A port connected to the device is not a trunk or hybrid port.
- The allowed VLAN list of the port connected to the device does not contain the user communication VLANs.
- The protocol-based VLAN function is disabled on a port.
- Packets match a VLAN assignment policy with a higher priority (for example, MAC VLAN, voice VLAN, or subnet-based VLAN) on the port, causing the failure of the protocol-based VLAN policy to take effect.

Contents

1 Configuring Private VLAN 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Packet Forwarding Rules 3
1.2 Restrictions and Guidelines 4
1.3 Configuration Task Summary 4
1.4 Configuring PVLAN and Layer 2 Association 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 5
1.4.3 Procedure 5
1.5 Configuring a Layer 3 Association for a PVLAN 6
1.5.1 Overview 6
1.5.2 Restrictions and Guidelines 6
1.5.3 Prerequisites 6
1.5.4 Procedure 6
1.6 Configuring an Isolated Port or a Community Port 7
1.6.1 Overview 7
1.6.2 Restrictions and Guidelines 7
1.6.3 Prerequisites 7
1.6.4 Procedure 7
1.7 Configuring a Promiscuous Port 8

1.7.1 Overview 8
1.7.2 Restrictions and Guidelines 8
1.7.3 Prerequisites 8
1.7.4 Procedure 8
1.8 Monitoring 9
1.9 Configuration Examples 9
1.9.1 Configuring PVLAN Across Layer 2 Devices 9
1.9.2 Configuring PVLAN on a Single Layer 3 Device 17

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 Layer 2. 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 a Layer 3 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.

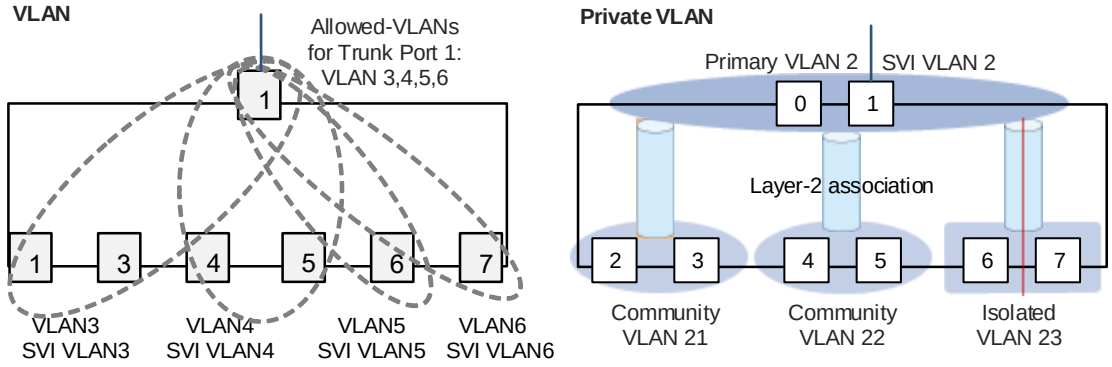
1.1.2 Basic Concepts

The PVLAN technology divides a Layer 2 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 ports. As shown in Figure 1-1, ports 0 and 1 within the primary VLAN belong to primary VLAN 2; and ports 2 and 3 belong to community VLAN 21. After a Layer 2 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 Layer 2 communication with each other.
- In a PVLAN, Layer 3 switch virtual interfaces (SVIs) can be created only in the primary VLAN, and Layer 3 SVIs cannot be created in secondary VLANs. You can make Layer 3 communication with the port in a primary VLAN through a port in the secondary VLAN only after a Layer 3 association is configured between the secondary VLAN and the primary VLAN. Otherwise, the hosts can make only Layer 2 communication.

Figure 1-1 Logic Diagram of PVLAN



2. Primary VLAN and Promiscuous Port

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 Packet Forwarding Rules

Table 1-1 lists packet forwarding rules between ports in a PVLAN and VLAN tag changes.

Table 1-1 Packet Forwarding Rules Between Different Types of Ports and VLAN Tag Changes

Input Port	Output Port	Packet Forwarding Rules and VLAN Tag Changes
Promiscuous Port	Promiscuous Port	Reachable, VLAN tag unchanged
	Community Port	Reachable, VLAN tag unchanged
	Isolated Port	Reachable, VLAN tag unchanged
	Trunk Port	Reachable, a primary VLAN tag added
Community Port	Promiscuous Port	Reachable, VLAN tag unchanged
	Community Port	● Reachable in the same community VLAN, VLAN tag unchanged ● Unreachable in different community VLANs
	Isolated Port	Unreachable
	Trunk Port	Reachable, a community VLAN tag added
Isolated Port	Promiscuous Port	Reachable, VLAN tag unchanged
	Community Port	Unreachable
	Isolated Port	Unreachable
	Trunk Port	Reachable. An isolated VLAN tag is added to an isolated VLAN packet and the packet is forwarded through isolated ports.
Trunk Port	Promiscuous Port	Reachable, VLAN tag removed
	Community Port	● 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
	Isolated Port	● Reachable in the primary VLAN, VLAN tag removed ● Unreachable in a community VLAN ● Unreachable in an isolated VLAN
	Trunk Port	Reachable, VLAN tag unchanged
Switch CPU	Promiscuous Port	Reachable, no VLAN tag

Input Port	Output Port	Packet Forwarding Rules and VLAN Tag Changes
	Community Port	Reachable, no VLAN tag
	Isolated Port	Reachable, no VLAN tag
	Trunk Port	Reachable, a primary VLAN tag added
	Isolated Trunk Port	Reachable, an isolated VLAN tag added

1.2 Restrictions and Guidelines

- You can only configure a Layer 2 Ethernet interface or a Layer 2 aggregated port as an isolated, community or promiscuous port within a PLVAN and add the port to the PVLAN.
- You can run the **show interface switchport** command to display the interface type. If the **Switchport** field corresponding to the interface is **enabled**, this interface is a Layer 2 interface. If the **Switchport** field corresponding to the interface is **disabled**, this interface is a Layer 3 interface.
- You can run the **switchport** command to configure the interface as a Layer 2 interface. Run the **no switchport mode** command to restore the Layer 2 interface mode to the default mode and run the **no switchport** command to configure a Layer 2 interface as a Layer 3 interface. When you configure an interface as a Layer 2 or 3 interface, all attributes of the interface are restored to the default values in this interface mode.

1.3 Configuration Task Summary

The configuration includes the following tasks:

(1) Configure PVLAN.

a Configuring PVLAN and Layer 2 Association

b Configuring a Layer 3 Association for a PVLAN

(2) Configure port types and add the ports to PVLAN pairs.

a Configuring an Isolated Port or a Community Port

b Configuring a Promiscuous Port

1.4 Configuring PVLAN and Layer 2 Association

1.4.1 Overview

The primary VLAN and secondary VLANs of a PVLAN cannot exist separately. You must add the secondary VLANs to the primary VLAN to form a Layer 2 association and multiple PVLAN pairs, which is also called PVLAN sub-domains.

You can add isolated ports and community ports to the primary VLAN and secondary VLANs only after a Layer 2 association is configured between the secondary VLANs and the primary VLAN. If you cancel a Layer 2 association, the PVLAN pairs, to which the isolated ports and promiscuous ports are added, are canceled as well.

After a Layer 2 association is configured between the secondary VLANs and the primary VLAN, you can configure a Layer 3 association so that the multiple secondary VLANs use the same IP gateway to save IP address resources.

Use the **private-vlan association** command to configure a Layer 2 association between the primary VLAN and the secondary VLANs.

1.4.2 Restrictions and Guidelines

- The PVLAN supports only host and promiscuous ports. Before you configure a common VLAN as a PVLAN, ensure that the ports in the PVLAN are valid. Otherwise, the configuration may fail. If a trunk, hybrid or uplink port exists in a common VLAN, the common VLAN can be configured as a PVLAN, but you are advised to remove the unused port from the PVLAN. If an access or dot1q-tunnel port exists in a common VLAN, the common VLAN cannot be configured as a PVLAN.
- **primary**: Configure a common VLAN as the primary VLAN of a PVLAN. A primary VLAN specifies a PVLAN. The device support creating multiple PVLANs and configuring multiple primary VLANs.
- **community**: Configure a common VLAN as a community VLAN. A Private VLAN has one or more community VLANs. Therefore, each primary VLAN can be associated with one or more community VLANs.
- **isolated**: Configure a common VLAN as an isolated VLAN. A Private VLAN has only one isolated VLAN. Therefore, each primary VLAN can be associated with only one isolated VLAN.
- *secondary-vlan-list* indicates a list of secondary VLANs. **add** *secondary-vlan-list* is used to associate with a secondary VLAN. **remove** *secondary-vlan-list* is used to remove the association specified by *secondary-vlan-list*.
- You cannot delete a PVLAN by using the **no vlan** command. You must run the **no private-vlan** { **community** | **isolated** | **primary** } command to restore a PVLAN to a common static VLAN, and be sure to keep the original PVLAN attributes unchanged.
- Before you modify PVLAN attributes of a port, you must restore the PVLAN to a common static VLAN and then configure new PVLAN attributes for the port. When you restore a PVLAN to a common static VLAN, all the associations in the PVLAN are canceled. You need to reconfigure associations for the PVLAN and add ports to the PVLAN.

1.4.3 Procedure

(1) Configure a secondary VLAN for a PVLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a secondary VLAN and enter the VLAN configuration mode.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Configure attributes of the secondary VLAN.

private-vlan { **community** | **isolated** }

A VLAN is a common VLAN and has no PVLAN attribute by default.

e Return to the global configuration mode.

exit

(2) Configure a primary VLAN for the PVLAN.

a Create a primary VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

Only VLAN 1 exists by default.

b Configure attributes of the primary VLAN.

private-vlan primary

A VLAN is a common VLAN and has no PVLAN attribute by default.

(3) Add the secondary VLAN to the primary VLAN to form a Layer 2 association.

private-vlan association { *secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list* }

No Layer 2 association is configured between the primary VLAN and the secondary VLANs by default.

1.5 Configuring a Layer 3 Association for a PVLAN

1.5.1 Overview

To enable hosts in a secondary VLAN domain to access an external network, configure a Layer 3 SVI for the primary VLAN, configure an IP address for the SVI, and then configure a Layer 3 association between the primary VLAN and the secondary VLAN on the SVI of the primary VLAN. Then, hosts in the secondary VLAN can make Layer 3 communication through the SVI of the primary VLAN. If no Layer 3 association is configured between the primary VLAN and the secondary VLAN, the hosts in the secondary VLAN cannot make Layer 3 communication.

You can use the **private-vlan mapping** command to configure/remove a Layer 3 association between the primary VLAN and the secondary VLAN.

1.5.2 Restrictions and Guidelines

- You can create an SVI only for a primary VLAN. Run the **interface vlan** *interface-number* command to create an SVI. The value of *interface-number* must be the VID of a primary VLAN.
- To configure an IPv4 address, see *Configuring IPv4 Basics*.
- To configure an IPv6 address, see *Configuring IPv6 Basics*.

1.5.3 Prerequisites

Create a PVLAN and a Layer 2 association between a secondary VLAN and the primary VLAN.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an SVI for the primary VLAN and enter the SVI configuration mode.

interface vlan *interface-number*

No SVI exists in a VLAN by default.

(4) Configure an IP address for the SVI.

ip address { *ipv4-address mask* | *ipv4-address/mask-length* }

An SVI has no IP address by default.

(5) Configure a Layer 3 association for the PVLAN.

private-vlan mapping { *secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list* }

No Layer 3 association is configured between the primary VLAN and the secondary VLANs by default.

1.6 Configuring an Isolated Port or a Community Port

1.6.1 Overview

After the primary VLAN and secondary VLAN as well as a Layer 2 association are configured, you need to configure ports connected to hosts. User ports are configured as host ports. If an enterprise has only one host, you can configure the user port as an isolated port and add the port to an isolated VLAN. If an enterprise has multiple hosts, you can configure the user ports as community ports and add the ports to a community VLAN. The host ports added to an isolated VLAN are isolated ports, and the host ports added to community VLANs are community ports.

1.6.2 Restrictions and Guidelines

- The Layer 2 interfaces connected to hosts must be configured as host ports before they are associated with PVLAN pairs to add the host ports to a secondary VLAN of a PVLAN.
- *primary-vlan-id* specifies the primary VLAN ID in a PVLAN pair. *secondary-vlan-id* specifies a secondary VLAN ID in a PVLAN pair. The VLANs specified by *primary-vlan-id* and *secondary-vlan-id* must be a PVLAN pair that has a Layer 2 association.
- One host port can be associated with only one PVLAN pair. To modify the association of a host port with a PVLAN pair, use the **no switchport private-vlan host-association** command to cancel the association between the host port and the PVLAN pair.

1.6.3 Prerequisites

- Configure an interface as a Layer 2 interface.

Create a PVLAN and a Layer 2 association between a secondary VLAN and the primary VLAN.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure a Layer 2 interface as a PVLAN host port.

switchport mode private-vlan host

A Layer 2 interface is an access port by default.

(5) Associate the host port with a PVLAN pair that has a Layer 2 association and add the host port to a secondary VLAN of the PLVAN.

switchport private-vlan host-association *primary-vlan-id secondary-vlan-id*

A port belongs to VLAN 1 and is not associated with a Layer 2 PVLAN pair by default.

1.7 Configuring a Promiscuous Port

1.7.1 Overview

To enable a port connected to an external network or a server to be accessible to community ports and isolated ports, configure the port as a promiscuous port so that uplink and downlink packets can be normally forwarded.

1.7.2 Restrictions and Guidelines

- You must configured a Layer 2 interface as a promiscuous port and then associate the promiscuous port with a PVLAN pair to add the port to the primary VLAN of the PLVAN.
- A promiscuous port can be associated with multiple PVLAN pairs that share the same primary VLAN. However, a host port can be associated with one PVLAN pair only.

1.7.3 Prerequisites

- Configure an interface as a Layer 2 interface.

Create a PVLAN and a Layer 2 association between a secondary VLAN and the primary VLAN.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure a Layer 2 interface as a PVLAN promiscuous port.

switchport mode private-vlan promiscuous

A Layer 2 interface is an access port by default.

(5) Associate the promiscuous port with one or more PVLAN pairs that have Layer 2 associations to add the port to the primary VLAN of the PLVAN.

switchport private-vlan mapping *primary-vlan-id* { *secondary-vlan-list* | **add** *secondary-vlan-list* | **remove** *secondary-vlan-list* }

A port belongs to VLAN 1 and is not associated with a Layer 2 PVLAN pair by default.

1.8 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 vlan private-vlan [**community** | **primary** | **isolated**]	Displays PVLAN configuration.

1.9 Configuration Examples

1.9.1 Configuring PVLAN Across Layer 2 Devices

1. Requirements

As shown in Figure 1-2, in the hosting service operation network, enterprise hosts are connected to the network through device A or device B. Main requirements are as follows:

- Hosts of an enterprise can communicate with each other but the host communication between enterprises is isolated. All enterprise hosts share the same gateway address and can communicate with the external network through this gateway address.

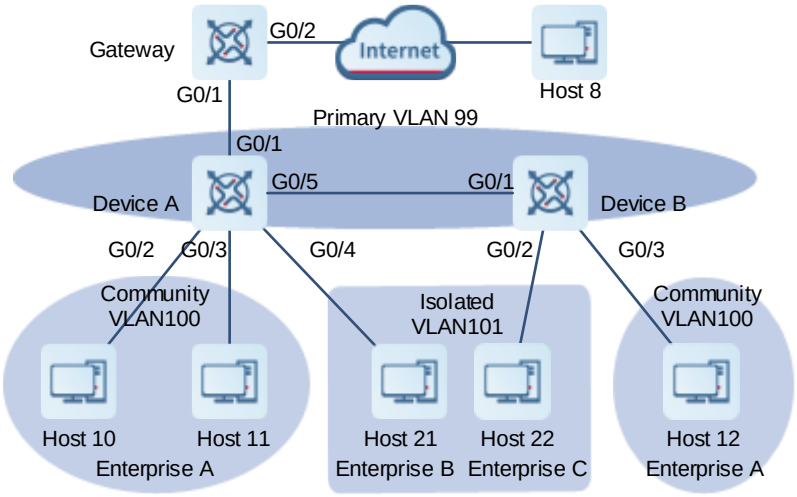
The deployment mode is as follows:

- Configure the PVLAN function on device A and device B and the interconnection ports are all trunk ports. 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 SVI of the primary VLAN 99. The external network perceives the primary VLAN 99 only and does not perceive secondary VLANs. Configure GigabitEthernet 0/1 of device A as a promiscuous port and connect this interface to the gateway. The promiscuous port only allows primary VLAN packets from the PVLAN to pass through and outputs untagged packets.
- GigabitEthernet 0/1 of the gateway can function as a trunk or hybrid port. Because packets forwarded by a promiscuous port are untagged, set the native VLAN of GigabitEthernet 0/1 of the gateway to the primary VLAN of the PVLAN.
- 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.

2. Topology

Figure 1-2 Topology of PVLAN Applied Across Layer 2 Devices



3. Notes

- Add all enterprise hosts to a PVLAN (primary VLAN 99). All enterprise hosts share the same SVI through this PVLAN to communicate with the external network. Enterprise A has multiple hosts. Assign the hosts to community VLAN 100 so that hosts in the enterprise can communicate with each other and the host communication between enterprises is isolated. Enterprise B and enterprise C has only one host each. Assign the hosts to isolated VLAN 101. The hosts in enterprise B and enterprise C cannot communicate with each other. Configure a PVLAN on Device A and Device B. The PVLAN contains one primary VLAN 99, one community VLAN 100, and one isolated VLAN 101.
- Configure a Layer 3SVI for the primary VLAN on Device A, and configure a Layer 3 association between the primary VLAN and the secondary VLANs.
- Configure GigabitEthernet 0/2-0/4 of Device A as host ports. Configure GigabitEthernet 0/2 and 0/3 of Device B as host ports.
- Configure GigabitEthernet 0/1 of Device A connected to a gateway as a promiscuous port. Only packets from the primary VLAN can pass through this port. No tag is carried when the promiscuous port outputs packets from the primary VLAN.
- Because the PVLAN runs across devices, the ports connecting different devices must be configured as trunk ports. Configure GigabitEthernet 0/5 of Device A and GigabitEthernet 0/1 of Device B as trunk ports. GigabitEthernet 0/1 of the gateway can be configured as a trunk port or hybrid port. Because packets forwarded by a promiscuous port do not carry tags, the native VLAN of GigabitEthernet 0/1 must be set to the primary VLAN of the PVLAN.

4. Procedure

(1) Configure a PVLAN and Layer 2 associations.

Configure a Layer 2 association between the secondary VLANs (VLAN 100 and VLAN 101) and the primary VLAN 99 on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 100
DeviceA(config-vlan)# private-vlan community
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 101
DeviceA(config-vlan)# private-vlan isolated
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 99
DeviceA(config-vlan)# private-vlan primary
DeviceA(config-vlan)# private-vlan association 100-101
DeviceA(config-vlan)# exit
```

Configure a Layer 2 association between the secondary VLANs (VLAN 100 and VLAN 101) and the primary VLAN 99 on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan 100
DeviceB(config-vlan)# private-vlan community
DeviceB(config-vlan)# exit
DeviceB(config)# vlan 101
DeviceB(config-vlan)# private-vlan isolated
DeviceB(config-vlan)# exit
DeviceB(config)# vlan 99
DeviceB(config-vlan)# private-vlan primary
DeviceB(config-vlan)# private-vlan association 100-101
DeviceB(config-vlan)# exit
```

(2) Configure a Layer 3 association for the PVLAN.

Configure an IP address and a mask for the Layer 3 SVI of the primary VLAN on Device A, and configure a Layer 3 association between the primary VLAN and the secondary VLANs.

```
DeviceA(config)# interface vlan 99
DeviceA(config-vlan)# ip address 192.168.99.1 255.255.255.0
DeviceA(config-vlan)# private-vlan mapping 100,101
DeviceA(config-vlan)# exit
```

(3) Add the host ports to the secondary VLANs.

Configure the ports of Device A connected to hosts as host ports and associate the ports with PVLAN pairs to add the ports to the secondary VLANs.

```
DeviceA(config)# interface range gigabitethernet 0/2-3
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode private-vlan host
DeviceA(config-if-range)# switchport private-vlan host-association 99 100
DeviceA(config-if-range)# exit
DeviceA(config)# interface gigabitethernet 0/4
```

```
DeviceA(config-if-GigabitEthernet 0/4)# switchport
DeviceA(config-if-GigabitEthernet 0/4)# switchport mode private-vlan host
DeviceA(config-if-GigabitEthernet 0/4)# switchport private-vlan
host-association 99 101
DeviceA(config-if-GigabitEthernet 0/4)# exit
```

Configure the ports of Device B connected to hosts as host ports and associate the ports with PVLAN pairs to add the ports to the secondary VLANs.

```
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# switchport
DeviceB(config-if-GigabitEthernet 0/2)# switchport mode private-vlan host
DeviceB(config-if-GigabitEthernet 0/2)# switchport private-vlan
host-association 99 101
DeviceB(config-if-GigabitEthernet 0/2)# exit
DeviceB(config)# interface gigabitethernet 0/3
DeviceB(config-if-GigabitEthernet 0/3)# switchport
DeviceB(config-if-GigabitEthernet 0/3)# switchport mode private-vlan host
DeviceB(config-if-GigabitEthernet 0/3)# switchport private-vlan
host-association 99 100
DeviceB(config-if-GigabitEthernet 0/3)# exit
```

(4) Configure GigabitEthernet 0/1 of Device A as a promiscuous port and associate the port with the primary VLAN 99 and the secondary VLANs 100 and 101 to add the port to the primary VLAN.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode private-vlan promiscuous
DeviceA(config-if-GigabitEthernet 0/1)# switchport private-vlan mapping 99 add
100-101
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

(5) Configure the ports connecting devices in the PVLAN as common trunk ports.

Configure GigabitEthernet 0/5 of Device A as a trunk port.

```
DeviceA(config)# interface gigabitethernet 0/5
DeviceA(config-if-GigabitEthernet 0/5)# switchport
 DeviceA(config-if-GigabitEthernet 0/5)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/5)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/5)# switchport trunk allowed vlan all
DeviceA(config-if-GigabitEthernet 0/5)# end
DeviceA# write
```

Configure GigabitEthernet 0/1 of Device B as a trunk port.

```
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)# switchport trunk native vlan 1
DeviceB(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
DeviceB(config-if-GigabitEthernet 0/1)# end
DeviceB# write
```

(6) Configure the downlink port GigabitEthernet 0/1 of the gateway as a trunk port and set the native VLAN of this port to the primary VLAN.

```
GW> enable
GW# configure terminal
GW(config)# interface gigabitethernet 0/1
GW(config-if-GigabitEthernet 0/1)# switchport
GW(config-if-GigabitEthernet 0/1)# switchport mode trunk
GW(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 99
GW(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
GW(config-if-GigabitEthernet 0/1)# end
GW# write
```

5. Verification

(1) Check whether the VLAN and port configurations are correct.

Check whether the VLAN and port configurations on Device A are correct. GigabitEthernet 0/1 is a promiscuous port and belongs to primary VLAN 99. GigabitEthernet 0/2 and GigabitEthernet 0/3 are community ports and belong to community VLAN 100. GigabitEthernet 0/4 is an isolated port and belongs to isolated VLAN 101. GigabitEthernet 0/5 is a trunk port and belongs to all VLANs. A Layer 3 SVI address is configured on Device A and the routing function is enabled.

```
DeviceA# show vlan private-vlan
VLAN  Type      Status   Routed    Ports                Associated VLANs
----  ----     -------   ------    ------------------     ------------------
99    primary    active   Enabled    Gi0/1, Gi0/5          100-101
100   community  active   Enabled    Gi0/2, Gi0/3, Gi0/5    99
101   isolated   active   Enabled    Gi0/4, Gi0/5          99
```

Check whether the VLAN and port configurations on Device B are correct.

```
DeviceB# show vlan private-vlan
VLAN  Type      Status   Routed    Ports                Associated VLANs
----  ----     -------   ------    ------------------     ------------------
99    primary    active   Disabled   Gi0/1                100-101
100   community  active   Disabled   Gi0/1, Gi0/3          99
101   isolated   active   Disabled   Gi0/1, Gi0/2          99
```

Check whether the gateway configuration is correct.

```
GW# show interface gigabitethernet 0/1 switchport
 Interface                    Switchport Mode     Access Native Protected VLAN
lists
 -------------------------------- ---------- --------- ------ ------ ---------
----------
 GigabitEthernet 0/1            enabled    TRUNK    1     99    Disabled  ALL
```

(2) Configure IP addresses and masks for hosts. To facilitate verification, add the hosts to the same network segment.

Configure an IP address and a mask for host 10 in the community VLAN.

```
Host10> enable
```

```
Host10# configure terminal
Host10(config)# interface gigabitethernet 0/1
Host10(config-if-GigabitEthernet 0/1)# no switchport
Host10(config-if-GigabitEthernet 0/1)# ip address 192.168.99.10 255.255.255.0
```

Configure an IP address and a mask for host 11 in the community VLAN.

```
Host11> enable
Host11# configure terminal
Host11(config)# interface gigabitethernet 0/1
Host11(config-if-GigabitEthernet 0/1)# no switchport
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.99.11 255.255.255.0
```

Configure an IP address and a mask for host 12 in the community VLAN.

```
Host12> enable
Host12# configure terminal
Host12(config)# interface gigabitethernet 0/1
Host12(config-if-GigabitEthernet 0/1)# no switchport
Host12(config-if-GigabitEthernet 0/1)# ip address 192.168.99.12 255.255.255.0
```

Configure an IP address and a mask for host 21 in the isolated VLAN.

```
Host21> enable
Host21# configure terminal
Host21(config)# interface gigabitethernet 0/1
Host21(config-if-GigabitEthernet 0/1)# no switchport
Host21(config-if-GigabitEthernet 0/1)# ip address 192.168.99.21 255.255.255.0
```

Configure an IP address and a mask for host 22 in the isolated VLAN.

```
Host22> enable
Host22# configure terminal
Host22(config)# interface gigabitethernet 0/1
Host22(config-if-GigabitEthernet 0/1)# no switchport
Host22(config-if-GigabitEthernet 0/1)# ip address 192.168.99.22 255.255.255.0
```

To simulate external network data, connect host 8 to the gateway interface GigabitEthernet 0/2 and add GigabitEthernet 0/2 to VLAN 99.

```
GW> enable
GW# configure terminal
GW(config)# interface gigabitethernet 0/2
GW(config-if-GigabitEthernet 0/2)# switchport
GW(config-if-GigabitEthernet 0/2)# switchport access vlan 99
```

Configure an address and a mask for host 8.

```
Host8> enable
Host8# configure terminal
Host8(config)# interface gigabitethernet 0/1
Host8(config-if-GigabitEthernet 0/1)# no switchport
Host8(config-if-GigabitEthernet 0/1)# ip address 192.168.99.8 255.255.255.0
```

(3) Check whether packets from the hosts in the PVLAN are forwarded in accordance with the forwarding rules of the PVLAN ports.

Hosts in the same community VLAN can communicate with each other even if the PVLAN is configured across devices.

```
Host10# ping 192.168.99.11
Sending 5, 100-byte ICMP Echoes to 192.168.99.11, 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.
Host10# ping 192.168.99.12
Sending 5, 100-byte ICMP Echoes to 192.168.99.12, 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 an isolated VLAN cannot communicate with each other.

```
Host21# ping 192.168.99.22
Sending 5, 100-byte ICMP Echoes to 192.168.99.22, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

Hosts in a community VLAN cannot communicate with hosts in an isolated VLAN.

```
Host10# ping 192.168.99.22
Sending 5, 100-byte ICMP Echoes to 192.168.99.22, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

Hosts in a community VLAN and hosts in an isolated VLAN can communicate with an external network through the promiscuous port and gateway.

```
Host10# ping 192.168.99.8
Sending 5, 100-byte ICMP Echoes to 192.168.99.8, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms.
Host22# ping 192.168.99.8
Sending 5, 100-byte ICMP Echoes to 192.168.99.8, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms.
```

6. Configuration Files

- Device A configuration file

```
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
```

```
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
switchport
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 99 add 100-101
!
interface GigabitEthernet 0/2
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/3
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/4
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/5
switchport
 switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface VLAN 99
 private-vlan mapping add 100,101
 ip address 192.168.99.1 255.255.255.0
```

- Device B configuration file

```
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
```

```
switchport
 switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/3
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
```

- Gateway configuration file

```
vlan range 1,99
!
interface GigabitEthernet 0/1
switchport
 switchport mode trunk
switchport trunk native vlan 99
switchport trunk allowed vlan only 1-4094
```

7. Common Errors

- No Layer 2 association is configured between the primary VLAN and the secondary VLANs of a PVLAN. As a result, a VLAN list fails to be added to an isolated port, a promiscuous port, or a community port when you configure the port.
- A host has been associated with a PVLAN pair when it is associated with another PVLAN pair, which will cause a configuration error.
- No Layer 3 association is configured for a PVLAN.

1.9.2 Configuring PVLAN on a Single Layer 3 Device

1. Requirements

As shown in Figure 1-3, in the hosting service operation network, enterprise hosts are connected to the network through the Layer 3 Device A. Main requirements are as follows:

- Hosts of an enterprise can communicate with each other but the host communication between enterprises is isolated.
- All enterprise hosts share the same gateway address and can communicate with the external network through this gateway address.
- All enterprise hosts can access the server.

The deployment mode is as follows:

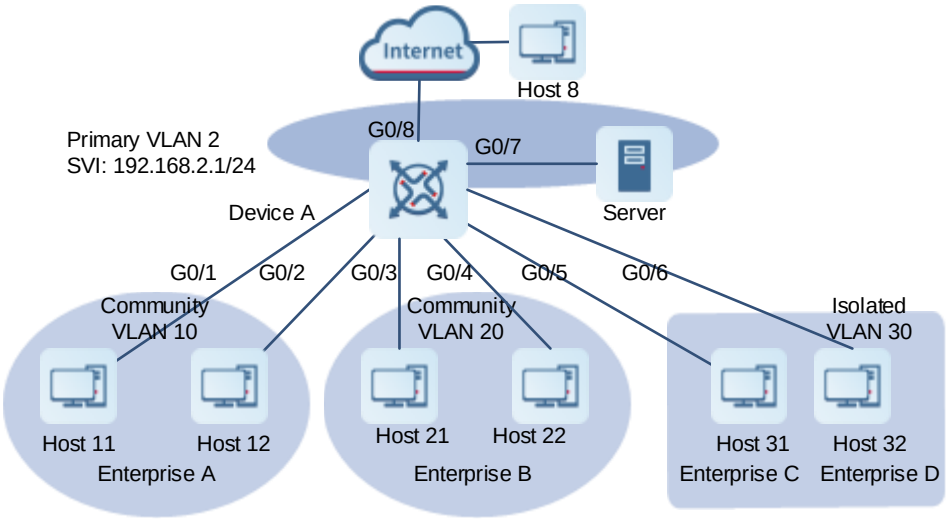
- Add all enterprise hosts to the same PVLAN (for example, primary VLAN 2). Assign hosts of enterprise A to community VLAN 10, hosts of enterprise B to community VLAN 20, and hosts of enterprises C and D to

isolated VLAN 30.

- Configure the SVI gateway (for example, 192.168.2.1/24) of the PVLAN on the Layer 3 device A and configure the mappings between the primary VLAN and the secondary VLANs on the Layer 3. Then, all enterprise hosts can communicate with the external network through this gateway address.
- Configure the port directly connected to the server as a promiscuous port. All enterprise hosts can communicate with the server through the promiscuous port.

2. Topology

Figure 1-3 Topology of PVLAN Applied on a Single Layer 3 Device



3. Notes

- Configure the PVLAN function on Device A. VLAN 2 is the primary VLAN. VLAN 10, VLAN 20, and VLAN 30 are secondary VLANs.
- 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 GigabitEthernet 0/8 of Device A that is connected to an external network as a promiscuous port. Set the IP address of the gateway SVI to 192.168.2.1/24 and configure a Layer 3 associations between the primary VLAN 2 and the secondary VLANs (VLAN 10, VLAN 20, and VLAN 30). All enterprise hosts can communicate with an external network based on this gateway IP address.

4. Procedure

(1) Configure a Layer 2 association between the primary VLAN and the secondary VLANs.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan 10
DeviceA(config-vlan)# private-vlan community
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 20
DeviceA(config-vlan)# private-vlan community
```

```
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 30
DeviceA(config-vlan)# private-vlan isolated
DeviceA(config-vlan)# exit
DeviceA(config)# vlan 2
DeviceA(config-vlan)# private-vlan primary
DeviceA(config-vlan)# private-vlan association 10,20,30
DeviceA(config-vlan)# exit
```

(2) Configure the ports connected to hosts as host ports and associate the ports with the primary VLAN and secondary VLANs to add the ports to the secondary VLANs.

```
DeviceA(config)# interface range gigabitethernet 0/1-2
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode private-vlan host
DeviceA(config-if-range)# switchport private-vlan host-association 2 10
DeviceA(config-if-range)# exit
DeviceA(config)# interface range gigabitethernet 0/3-4
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode private-vlan host
DeviceA(config-if-range)# switchport private-vlan host-association 2 20
DeviceA(config-if-range)# exit
DeviceA(config)# interface range gigabitethernet 0/5-6
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode private-vlan host
DeviceA(config-if-range)# switchport private-vlan host-association 2 30
DeviceA(config-if-range)# exit
```

(3) Configure GigabitEthernet 0/7 connected to the server as a promiscuous port and associate the port with the primary VLAN and the secondary VLANs to add the port to the primary VLAN.

```
DeviceA(config)# interface gigabitethernet 0/7
DeviceA(config-if-GigabitEthernet 0/7)# switchport
DeviceA(config-if-GigabitEthernet 0/7)# switchport mode private-vlan promiscuous
DeviceA(config-if-GigabitEthernet 0/7)# switchport private-vlan mapping 2
10,20,30
DeviceA(config-if-GigabitEthernet 0/7)# exit
```

(4) Configure GigabitEthernet 0/8 connected to an external network as a promiscuous port and associate the port with the primary VLAN and the secondary VLANs to add the port to the primary VLAN.

```
DeviceA(config)# interface gigabitethernet 0/8
DeviceA(config-if-GigabitEthernet 0/8)# switchport
DeviceA(config-if-GigabitEthernet 0/8)# switchport mode private-vlan promiscuous
DeviceA(config-if-GigabitEthernet 0/8)# switchport private-vlan mapping 2
10,20,30
DeviceA(config-if-GigabitEthernet 0/8)# exit
```

(5) Create an SVI for the primary VLAN, configure an SVI address, and configure a Layer 3 association for the PVLAN.

```
DeviceA(config)# interface vlan 2
```

```
DeviceA(config-if-VLAN 2)# ip address 192.168.2.1 255.255.255.0
DeviceA(config-if-VLAN 2)# private-vlan mapping 10,20,30
DeviceA(config-if-VLAN 2)# end
DeviceA# write
```

5. Verification

(1) Check whether the PVLAN and port configurations are correct.

```
DeviceA# show vlan private-vlan
VLAN   Type      Status   Routed   Ports         Associated VLANs
-----  ---------  -------  -------  ------------   -------------------
2     primary    active   Enabled  Gi0/7, Gi0/8   10,20,30
10    community  active   Enabled  Gi0/1, Gi0/2    2
20    community  active   Enabled  Gi0/3, Gi0/4    2
30    isolated   active   Enabled  Gi0/5, Gi0/6    2
```

(2) Configure IP addresses and masks for hosts.

Configure an IP address and a mask for host 11.

```
Host11> enable
Host11# configure terminal
Host11(config)# interface gigabitethernet 0/1
Host11(config-if-GigabitEthernet 0/1)# no switchport
Host11(config-if-GigabitEthernet 0/1)# ip address 192.168.2.11 255.255.255.0
```

Configure an IP address and a mask for host 12.

```
Host12> enable
Host12# configure terminal
Host12(config)# interface gigabitethernet 0/1
Host12(config-if-GigabitEthernet 0/1)# no switchport
Host12(config-if-GigabitEthernet 0/1)# ip address 192.168.2.12 255.255.255.0
```

Configure an IP address and a mask for host 21.

```
Host21> enable
Host21# configure terminal
Host21(config)# interface gigabitethernet 0/1
Host21(config-if-GigabitEthernet 0/1)# no switchport
Host21(config-if-GigabitEthernet 0/1)# ip address 192.168.2.21 255.255.255.0
```

(3) Check whether packets from the hosts in the PVLAN are forwarded in accordance with the forwarding rules of the PVLAN ports.

Hosts in the same community VLAN can communicate with each other. Hosts in different community VLANs cannot communicate with each other.

```
Host11# ping 192.168.2.12
Sending 5, 100-byte ICMP Echoes to 192.168.2.12, 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.
```

```
Host11# ping 192.168.2.21
Sending 5, 100-byte ICMP Echoes to 192.168.2.21, timeout is 2 seconds:
  < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
```

Hosts in an isolated VLAN cannot communicate with each other (the specific process is omitted).

Hosts in a community VLAN cannot communicate with hosts in an isolated VLAN (the specific process is omitted).

Hosts in a community VLAN and hosts in an isolated VLAN can communicate with an external network through the promiscuous port (the specific process is omitted).

Promiscuous ports can communicate with each other (the specific process is omitted).

6. Configuration Files

Device A configuration file

```
vlan 2
 private-vlan primary
 private-vlan association add 10,20,30
!
vlan 10
 private-vlan community
!
vlan 20
 private-vlan community
!
vlan 30
 private-vlan isolated
!
interface GigabitEthernet 0/1
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/2
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/3
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/4
switchport
switchport mode private-vlan host
```

```
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
switchport
switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
switchport
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
switchport
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 2 add 10,20,30
!
interface GigabitEthernet 0/8
switchport
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
private-vlan mapping add 10,20,30
ip address 192.168.2.1 255.255.255.0
```

7. Common Errors

- No Layer 2 association is configured between the primary VLAN and the secondary VLANs of a PVLAN. As a result, configuring a Layer 3 association fails.
- No Layer 3 association is configured. As a result, hosts cannot communicate with the external network.
- The ports connecting to the server and the external network are not configured as promiscuous ports. Therefore, uplink and downlink configurations are asymmetric, causing a packet forwarding failure.

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 Layer 2 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 Layer 3 Communication for a Super-VLAN....7
1.4.1 Overview....7
1.4.2 Restrictions and Guidelines....7
1.4.3 Procedure....8
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....9
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 Layer 3 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 Layer 3 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 Layer 2. Each subnet must be assigned with a gateway IP address to implement inter-VLAN Layer 3 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.

Layer 2 isolation is implemented by sub-VLANs, and Layer 3 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 Layer 3 attributes of a common VLAN.

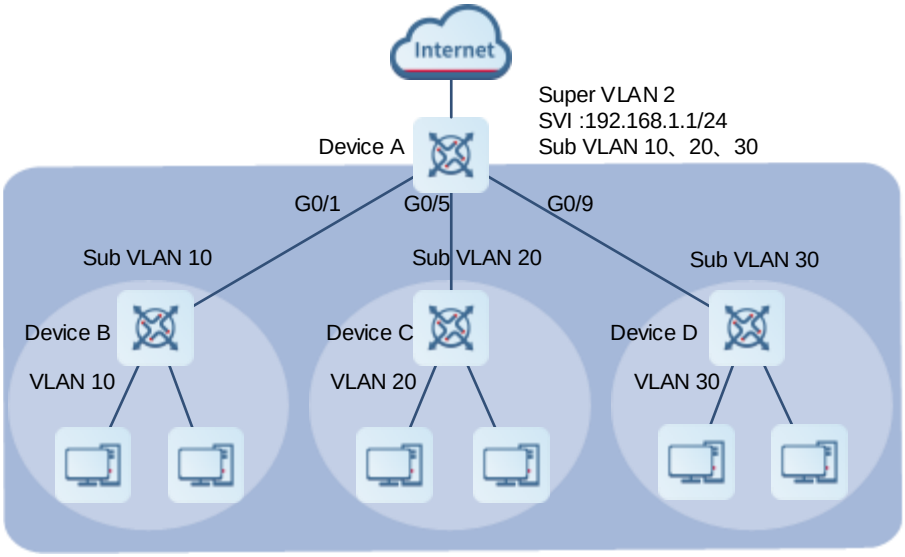
- Sub-VLAN

Each sub-VLAN is an independent broadcast domain, and is isolated from other sub-VLANs at Layer 2. 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 Layer 2 attributes of a common VLAN. To implement Layer 3 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 Layer 2 through sub-VLANs and make Layer 3 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 Layer 2 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 Layer 3 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 Layer 2 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 Layer 2 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 Layer 2 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 Layer 2 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 Layer 3. 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 Layer 3 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 Layer 2 Communication

Super-VLAN works at Layer 3. The SVI of a super-VLAN is used as a gateway only in Layer 3 communication across broadcast domains (across network segments or in the same network segment). The VLAN ID of a super-VLAN is not used in Layer 2 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 Layer 2 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 Layer 2 Association for a

b Configuring Layer 3 Communication for a

c (Optional) Configuring an IP Address Range for a

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 Layer 2 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 Layer 2 communication with each other but are Layer 2 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 Layer 3 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

No super-VLAN is configured by default.

(4) Add the common VLAN to the super-VLAN to make the common VLAN a sub-VLAN of the super-VLAN.

subvlan *vlan-id-list*

No common VLAN is added to a super-VLAN as a sub-VLAN by default.

1.4 Configuring Layer 3 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 a Layer 3 SVI can be configured for the super-VLAN. IP addresses must be configured for Layer 3 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 Layer 3 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.
- In the **interface vlan** *interface-number* command, *interface-number* indicates the SVI number, which must be the ID of the VLAN to which the SVI belong. The value range is 1-4094.
- When you configure an SVI for a super-VLAN, the system assigns a Layer 3 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 Layer 3 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.
- To configure an IPv4 address, see *Configuring IPv4*.
- To configure an IPv6 address, see *Configuring IPv6*.

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 *interface-number*

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 { *ipv4-address mask* | *ipv4-address/mask-length* }

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 Layer 3 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 Layer 3 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 the IP address range for users in the sub-VLAN.

subvlan-address-range *start-ipv4-address end-ipv4-address*

No IP address range is configured for users in the 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 [**id** *super-vlan-id*]	Displays the configuration of super-VLAN and sub-VLAN.
debug bridge svlan	Debugs the super-VLAN function.

1.8 Configuration Examples

1.8.1 Configuring Super-VLAN

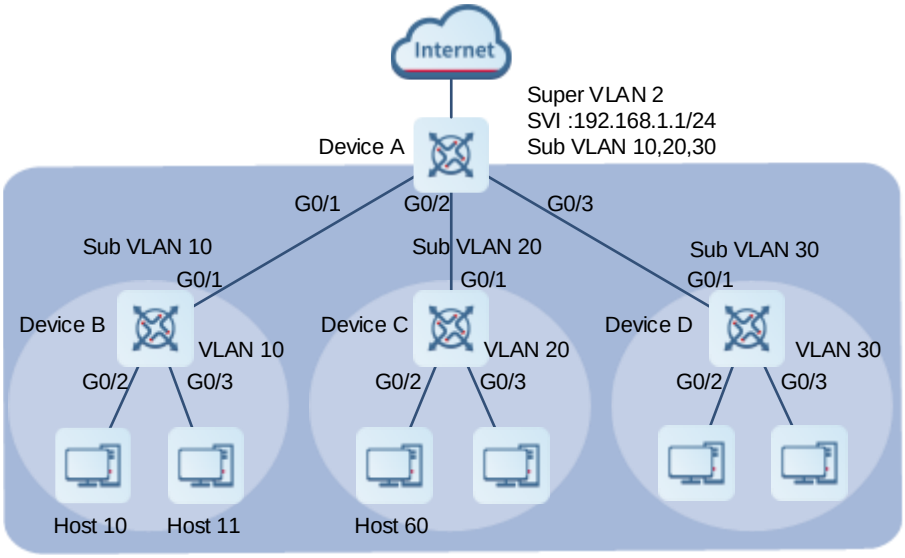
1. Requirements

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, 0/2, and 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(config-if-range)# switchport trunk native vlan 1
DeviceA(config-if-range)# switchport trunk allowed vlan all
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 Layer 2 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 Layer 3 communication but are isolated at Layer 2.

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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094

!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
```

```
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
switchport mode access
switchport access vlan 10
!
interface GigabitEthernet 0/3
switchport
switchport mode access
switchport access vlan 10
```

- Device C configuration file

```
vlan range 1,20
!
interface GigabitEthernet 0/1
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
switchport mode access
switchport access vlan 20
!
interface GigabitEthernet 0/3
switchport
switchport mode access
switchport access vlan 20
```

- Device D configuration file

```
vlan range 1,30
```

```
!
interface GigabitEthernet 0/1
switchport switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094!
interface GigabitEthernet 0/2
switchport
switchport mode access switchport access vlan 30
!
interface GigabitEthernet 0/3
switchport
switchport mode access
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 Layer 3 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 Restrictions and Guidelines....6
1.3 Configuration Task Summary....7
1.4 Configuring a Voice VLAN....7
1.4.1 Overview....7
1.4.2 Restrictions and Guidelines....7
1.4.3 Procedure....8
1.5 Configuring a Voice VLAN OUI....8
1.5.1 Overview....8
1.5.2 Restrictions and Guidelines....9
1.5.3 Procedure....9
1.6 Configuring a Voice Traffic Priority for a Voice VLAN....9
1.6.1 Overview....9
1.6.2 Restrictions and Guidelines....10
1.6.3 Prerequisites....10

1.6.4 Procedure....10
1.7 Configuration Aging Time for a Voice VLAN....10
1.7.1 Overview....10
1.7.2 Restrictions and Guidelines....10
1.7.3 Procedure....11
1.8 Configuring Security Mode for a Voice VLAN....11
1.8.1 Overview....11
1.8.2 Restrictions and Guidelines....11
1.8.3 Procedure....11
1.9 Configuring the Device to Automatically Add a Port to a Voice VLAN to Transmit Tagged Voice Traffic....11
1.9.1 Overview....11
1.9.2 Restrictions and Guidelines....11
1.9.3 Prerequisites....12
1.9.4 Procedure....12
1.10 Manually Adding a Port to a Voice VLAN to Transmit Tagged Voice Traffic....13
1.10.1 Overview....13
1.10.2 Restrictions and Guidelines....13
1.10.3 Prerequisites....13
1.10.4 Procedure....13
1.11 Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic....14
1.11.1 Overview....14
1.11.2 Restrictions and Guidelines....14
1.11.3 Prerequisites....15
1.11.4 Procedure....15

1.12 Configuring LLDP to Deliver a Voice VLAN Policy 15
1.12.1 Overview 15
1.12.2 Restrictions and Guidelines 15
1.12.3 Prerequisites 16
1.12.4 Procedure 16
1.13 Monitoring 17
1.14 Configuration Examples 17
1.14.1 Configuring a Port to Transmit Tagged Voice Traffic in Automatic Mode 17
1.14.2 Configuring a Port to Transmit Untagged Voice Traffic in Manual Mode 21
1.14.3 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.

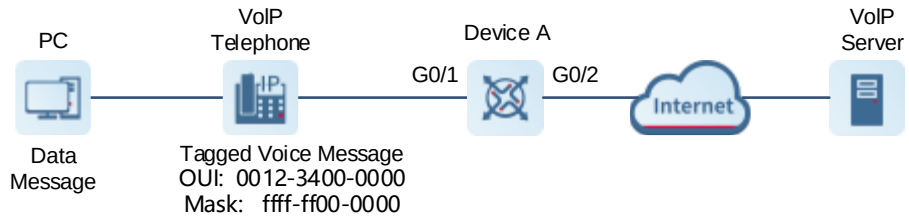
1.1.4 Work Mode of the Voice VLAN

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

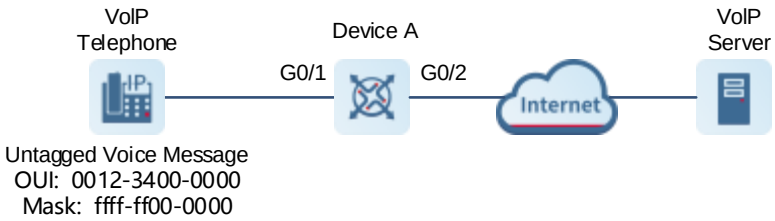
- In automatic mode, ports are automatically added to and removed from a voice VLAN. You are not allowed to manually add ports to a voice VLAN. Before you enable the voice VLAN function on a port, remove the voice VLAN from the allowed static VLAN list of the port to prevent the port from staying in 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.

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. Both 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

Port Type	Mode	Supported Work Mode and Configuration Requirement
	Automatic	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.
	Manual	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.

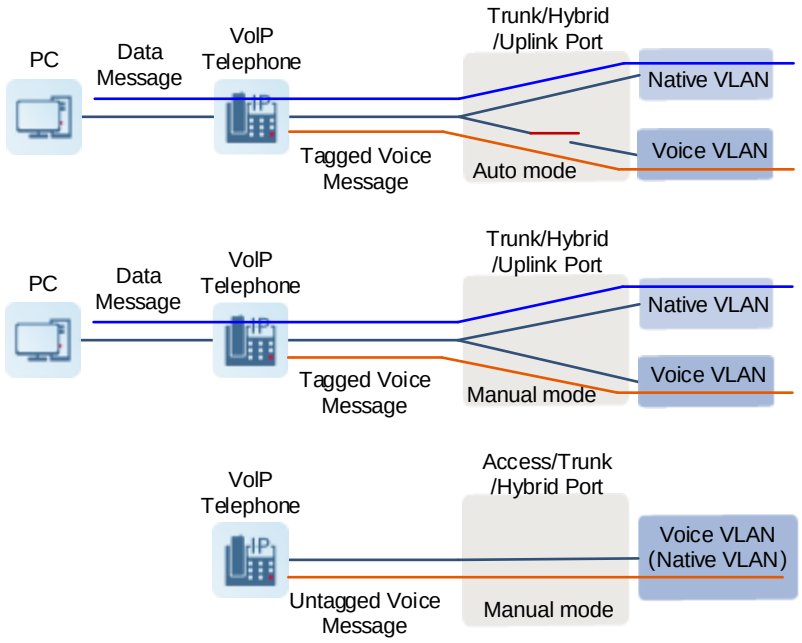
Port Type	Mode	Supported Work Mode and Configuration Requirement
Access Promiscuous Host	N/A	The access ports, promiscuous ports of PVLAN, and host ports do not support tagged voice traffic.

Table 1-2 Work Modes for Untagged Voice Traffic

If the voice traffic is untagged, the device supports only the manual mode.

Port Type	Mode	Supported Work Mode and Configuration Requirement
Access	Manual	The voice VLAN is the VLAN to which the access port belongs.
Host	Manual	The voice VLAN is the secondary VLAN (isolated or community VLAN) of a host port.
Promiscuous	Manual	The voice VLAN is the primary VLAN of a promiscuous port.
Trunk	Manual	The voice VLAN is the native VLAN of an access port and the port allows packets with the native VLAN ID to pass through.
Hybrid	Manual	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	N/A	An uplink port does not forward untagged packets. Therefore, when the voice traffic is untagged, the port cannot be configured as an uplink port.

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 Restrictions and Guidelines

- Voice VLAN can only be enabled on Layer 2 Ethernet interfaces (Access ports, Trunk port, Hybrid port,

Uplink port, PVLAN Host port and Promiscuous port), but not on the aggregate interface or Layer 3 interface.

- You can use the **show interface switchport** command to view the interface type. If the Switchport field corresponding to the interface is "enabled", it means that the interface is a Layer 2 interface. If the Switchport field corresponding to the interface is "disabled", it means that the interface is a Layer 3 interface.
- You can run the **switchport** command to configure the interface as a Layer 2 interface. First, use the **no switchport mode** command to restore the Layer 2 interface mode to the default value, and then use the **no switchport** command to configure the Layer 2 interface as a Layer 3 interface. When the Layer 2/Layer 3 interface mode is changed, all properties of the interface is restored to the default values of the interface type.

1.3 Configuration Task Summary

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

1.4 Configuring a Voice VLAN

1.4.1 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.

1.4.2 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.

1.4.3 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.

1.5 Configuring a Voice VLAN OUI

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.6 Configuring a Voice Traffic Priority for a Voice VLAN

1.6.1 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 QoS*.

1.6.2 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**.

1.6.3 Prerequisites

- Configure an interface connected to an audio deice as a Layer 2 interface.

A voice VLAN has been configured. An OUI has been configured.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) 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.

(4) Enter the Layer 2 Ethernet interface configuration mode to configure an interface connected to a voice device.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(5) 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.

1.7 Configuration Aging Time for a Voice VLAN

1.7.1 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.

1.7.2 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.

1.7.3 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.

1.8 Configuring Security Mode for a Voice VLAN

1.8.1 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.

1.8.2 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.

1.8.3 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.

1.9 Configuring the Device to Automatically Add 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

- 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.

1.9.3 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) Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(3) Configure the user port as a trunk port.

switchport mode trunk

An interface works in access mode by default.

(4) 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.

(5) 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 except *voice-vlan-id*

The default allowed VLANs of a trunk port are VLANs 1 to 4094.

(6) 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.

(7) 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 Tagged 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

- 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.

1.10.3 Prerequisites

Configure a voice VLAN.

1.10.4 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) Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(3) Configure the user port as a trunk port.

switchport mode trunk

An interface works in access mode by default.

(4) 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.

(5) 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.

(6) Configure the voice VLAN to work in manual mode.

no voice vlan mode auto

A voice VLAN works in automatic mode by default.

(7) 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 Manually Adding a Port to a Voice VLAN to Transmit Untagged Voice Traffic

1.11.1 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.

1.11.2 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.
- Taking the access port as an example, 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.

1.11.3 Prerequisites

Configure a voice VLAN.

1.11.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(4) Configure the user port as an access port.

switchport mode access

An interface works in access mode by default.

(5) 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.

(6) Configure the voice VLAN to work in manual mode.

no voice vlan mode auto

A voice VLAN works in automatic mode by default.

(7) Enable the voice VLAN function on the user port.

voice vlan enable

The voice VLAN function is disabled on a port by default.

1.12 Configuring LLDP to Deliver a Voice VLAN Policy

1.12.1 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.

1.12.2 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 Layer 2 Ethernet interface configuration mode to delete an LLDP network policy.
- For more information about command description, see *Configuring LLDP*.

1.12.3 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.

1.12.4 Procedure

(1) Create an LLDP network policy and enter the LLDP Network Policy 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 voice VLAN policy to enable the VoIP telephone to send tagged frames.

  { **voice** | **voice-signaling** } **vlan** { *voice-vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]

  No voice VLAN policy is configured by default.

- Configure a voice VLAN 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 an interface to allow advertising the Network Policy TLV.

a Return to the global configuration mode.

exit

b Enter the Layer 2 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

c Configure the interface to allow advertising the Network Policy TLV.

lldp tlv-enable med-tlv network-policy profile *profile-num*

The port is allowed to advertise the Network Policy TLV by default.

1.13 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.

1.14 Configuration Examples

1.14.1 Configuring a Port to Transmit Tagged Voice Traffic in Automatic Mode

1. Requirements

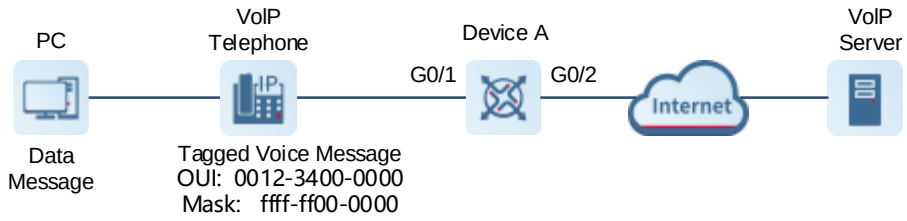
Each office staff member is assigned an Ethernet port. This port is used for service communication of a PC and voice communication of a VoIP telephone.

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 *Configuring IEEE 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
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 except 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
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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         5     Disabled  1,3-4094
GigabitEthernet 0/2   enabled    TRUNK         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
 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
```

```
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

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.

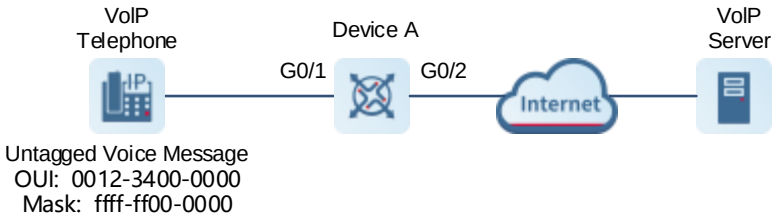
1.14.2 Configuring a Port to Transmit Untagged Voice Traffic in Manual Mode

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
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
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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# show interface switchport
Interface           Switchport Mode     Access Native Protected VLAN lists
-------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled    Access    2      1      Disabled  ALL
GigabitEthernet 0/2   enabled    TRUNK          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
switchport mode access
 switchport access vlan 2
 no voice vlan mode auto
 voice vlan enable
mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

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.

1.14.3 Configuring Isolation of Untagged Voice Traffic from Data Traffic

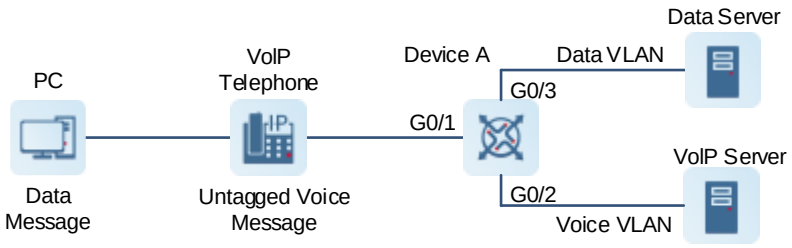
1. Requirements

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
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
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode access
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
DeviceA(config-if-GigabitEthernet 0/3)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/3)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan except 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
switchportswitchport 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
switchport mode access
switchport access vlan 2
!
interface GigabitEthernet 0/3
switchportswitchport mode trunk
switchport trunk native vlan 1switchport 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 4
1.1.6 Protocols and Standards 6
1.2 Restrictions and Guidelines 6
1.3 Configuration Task Summary 6
1.4 Configuring Basic Features 7
1.4.1 Overview 7
1.4.2 Restrictions and Guidelines 7
1.4.3 Prerequisites 8
1.4.4 Procedure 8
1.5 Configure GVRP Advertising Mode 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 Configure GVRP Registration Mode 9
1.6.1 Overview 9

1.6.2 Restrictions and Guidelines 10
1.6.3 Prerequisites 10
1.6.4 Procedure 10
1.7 Configuring GVRP BPDU Tunnels 10
1.7.1 Overview 10
1.7.2 Restrictions and Guidelines 11
1.7.3 Prerequisites 11
1.7.4 Procedure 11
1.8 Configuring Transparent Transmission of GVRP BPDU 11
1.8.1 Overview 11
1.8.2 Restrictions and Guidelines 12
1.8.3 Procedure 12
1.9 Monitoring 12
1.10 Configuration Examples 13
1.10.1 Configuring Basic Functions of GVRP 13
1.10.2 Configuring GVRP BPDU Tunnels 18

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 regularly collects or does not collect VLAN information of the local port according to the advertising mode of the port (**Normal** or **Non-Applicant**).

- **Normal** mode: A device collects the VLAN information, and encapsulates it in GVRP packets, and sends the packets to the peer device to externally advertise its VLAN information, including dynamic and static VLAN information. On such a basis, the peer device determines the VLAN to be created.
- **Non-Applicant** mode: A device does not collect the VLAN information or advertise its VLAN information.

3. GVRP Registration Mode

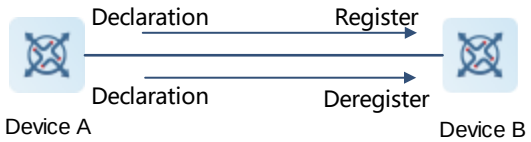
After receiving GVRP packets from the interconnected trunk port, the peer device parses the VLAN information and decides to process or not to process the VLAN information according to the port registration mode (**Normal** or **Disabled**).

- **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.

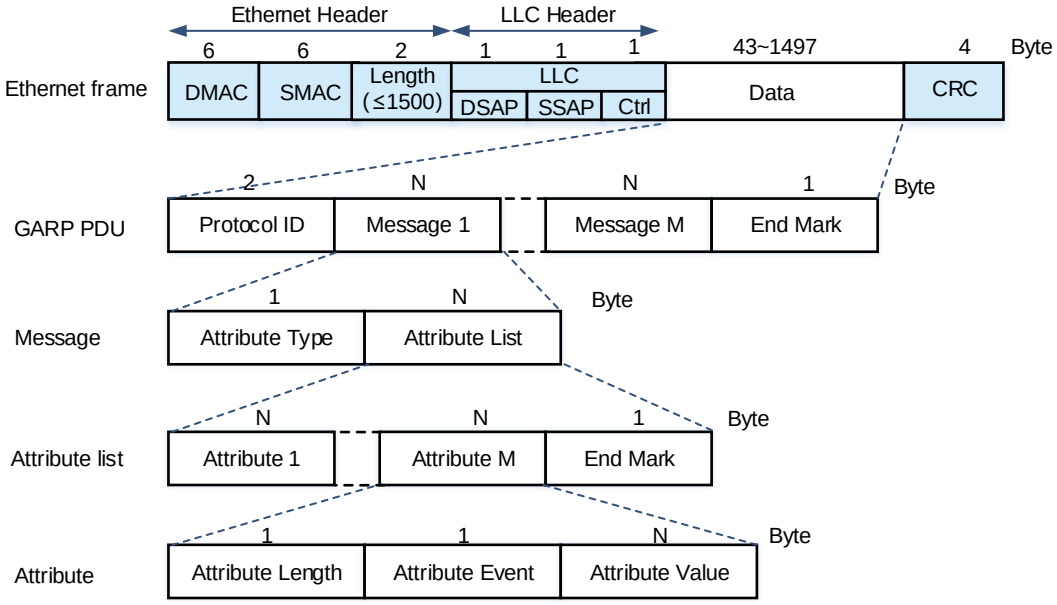
- LeaveAll timer

  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 1 to M (M is a positive integer) messages. 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 1 to M (M is a positive integer) 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.
Attribute Event	1	Indicates the event type described by the attribute. 0x00: LeaveAll Event 0x01: JoinEmpty Event 0x02: JoinIn Event 0x03: LeaveEmpty Event 0x04: LeaveIn Event 0x05: Empty Event

Field	Number of Bytes	Description
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, 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 Restrictions and Guidelines

- GVRP function can only be enabled on Trunk ports. Only Layer 2 Ethernet interfaces and Layer 2 aggregate interface can be configured as Trunk ports.
- You can use the **show interface switchport** command to view the interface type. if the **Switchport** field corresponding to the interface is "enabled", it means that the interface is a Layer 2 interface. If the Switchport field corresponding to the interface is "disabled", it means that the interface is a Layer 3 interface.
- You can use the **switchport** command to configure the interface as a Layer 2 interface. Use the **no switchport mode** command to restore the Layer 2 interface mode to the default value, and then use the **no switchport** command to configure the Layer 2 interface as a Layer 3 interface. When the Layer 2/Layer 3 interface mode is changed, all properties of the interface will be restored to the default values of the interface type.

1.3 Configuration Task Summary

- Configuring GVRP includes the following tasks:
- When the GVRP function is enabled, the configuration includes the following tasks:
  - a Configuring Basic Features
  - b (Optional) Configuring GVRP advertising mode
  - c (Optional) Confgiruing GVRP registration mode
  - d (Optional) Configuring GVRP BPDU Tunnels
- When the GVRP function is disabled, the configuration includes the following task:
  - (Optional) Configuring Transparent Transmission of GVRP BPDU

1.4 Configuring Basic Features

1.4.1 Overview

When the GVRP function is enabled, the device can send GVRP packets containing the VLAN information, 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. When the GVRP function is disabled, the device will not send or handle GVRP packets containing the VLAN information.

Dynamic VLAN creation must be enabled. When the VLAN indicated in the packet received by the port (only JoinIn and JoinEmpty) does not exist on the local device, GVRP may create this VLAN. If this function is enabled, when the device receives the Join message from GVRP, a VLAN will be created dynamically.

1.4.2 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.
  - The parameters of a dynamic VLAN created through GVRP cannot be modified manually.
- 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.
  - 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.

1.4.3 Prerequisites

- Configure the interface as a Layer 2 interface.

1.4.4 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 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 time interval for the port to send a LeaveAll message is 10,000 ms.

a Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

b Configure the Layer 2 interface as a trunk port (global GVRP function only takes effect on a trunk port).

switchport mode trunk

A Layer 2 interface works in access mode by default.

c Return to the global configuration mode.

exit

(5) Enable the GVRP function globally.

gvrp enable

The GVRP function is disabled by default.

1.5 Configure GVRP Advertising Mode

1.5.1 Overview

On the device with GVRP enabled, the Trunk port collects or does not collect VLAN information of the port regularly according to the port's notification mode (Normal or Non Application). You can use this function to configure the notification mode of the interface.

- Normal: Collect VLAN information, encapsulate these VLAN information in GVRP message, send notification to the peer device, and externally notify the VLAN information on the device, including dynamic

and static VLAN information, according to which the peer device determines the VLAN to be created.

- Non-Applicant: Do not collect the VLAN information of local port, and do not notify the VLAN information on local device.

1.5.2 Restrictions and Guidelines

- Use the **gvrp applicant state normal** command to enable the configuration to collect port VLAN information and send notifications.
- Use the **gvrp applicant state non-applicant** command to configure not to collect port VLAN information and not send notifications.

1.5.3 Prerequisites

- The interface is configured as a Layer 2 interface.
- Basic functions of GVRP are configured, including: enabling the dynamic VLAN creation function, configuring the Layer 2 interface as a Trunk port, and enabling the GVRP function globally.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 link aggregation configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the advertising mode on the interface.

gvrp applicant state { **normal** | **non-applicant** }

By default, the port advertising mode is Normal, the notification will be sent.

1.6 Configure GVRP Registration Mode

1.6.1 Overview

After receiving the GVRP message from the interconnected Trunk port, the peer device parses the VLAN information and chooses to process or not process the VLAN information according to the port registration mode (Normal or Disabled). You can use this function to configure the registration mode of the interface.

- Normal: Process VLAN information, dynamically create a non-existent VLAN and add the port receiving the message to the VLAN, or exit the VLAN.
- Disabled: The VLAN information in the message is not processed.

These two registration modes will not affect the static VLAN on the port. The static VLAN created by the user is always a Fixed Registrar.

1.6.2 Restrictions and Guidelines

- Use the **gvrp registration mode normal** command to allow dynamically create, register, or unregister VLANs on a port.
- Use the **gvrp register mode disable** command to disallow dynamically create, register, or unregister VLANs on a port.
- If enabled, it creates a dynamic VLAN after receiving the peer VLAN information. If disabled, when GVRP message is received, dynamic VLAN will not be added.

1.6.3 Prerequisites

- The interface is configured as a Layer 2 interface.
- Basic functions of GVRP are configured, including: enabling the dynamic VLAN creation function, configuring the Layer 2 interface as a Trunk port, and enabling the GVRP function globally.

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.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 link aggregation configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the registration mode of the port.

gvrp registration mode { **normal** | **disable** }

By default, the port registration mode is Normal, that is, the VLAN information is dynamically updated.

1.7 Configuring GVRP BPDU Tunnels

1.7.1 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 on the interface connected to the user network, 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.

1.7.2 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 Layer 2 Ethernet interface configuration mode or the Layer 2 link aggregation 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.

1.7.3 Prerequisites

- The interface connecting the user network is configured as a Layer 2 interface.
- The interface connecting the user network is configured as a Dot1q-tunnel interface.
- The QinQ encapsulation strategy is configured on the interface connecting to the user network.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (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.

(4) Enable the GVRP BPDU tunnel function globally.

l2protocol-tunnel gvrp

The global GVRP BPDU tunnel function is disabled by default.

(5) Enter the interface configuration mode to configure the interface connecting to the user network.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 link aggregation configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(6) Enable GVRP BPDU tunnel function on the interface.

l2protocol-tunnel gvrp enable

By default, GVRP BPDU tunnel function of the interface is disabled.

1.8 Configuring Transparent Transmission of GVRP BPDU

1.8.1 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 on interface connecting two devices to allow the interface to forward the packets with the destination MAC address of 0180.c200.0006.

1.8.2 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.

1.8.3 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.

1.9 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.

1.10 Configuration Examples

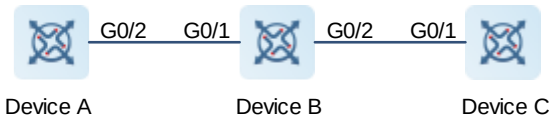
1.10.1 Configuring Basic Functions of GVRP

1. Requirements

As indicated in Figure 1-3, The GVRP function is enabled in a topology to dynamically maintain the VLANs and the VLAN-port relationship.

2. Topology

Figure 1-3 Topology of GVRP Basic Functions



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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
DeviceB(config-if-range)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
DeviceC(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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 interface 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     Disabled  ALL
```

Only a static VLAN exists on Device B; the interconnection interface 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     Disabled  ALL
GigabitEthernet 0/2       enabled    TRUNK          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     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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- Device B configuration file

```
gvrp enable
```

```
gvrp dynamic-vlan-creation enable
!
vlan range 1
!
interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- Device C configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,11-20
!
interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

7. Common Errors

- The interconnection interface of devices are not in trunk mode.
- The permitted VLAN list of the interconnection interface of devices does not contain the user communication VLANs.
- The GVRP advertising mode and registration mode of trunk ports are not set to **Normal**.

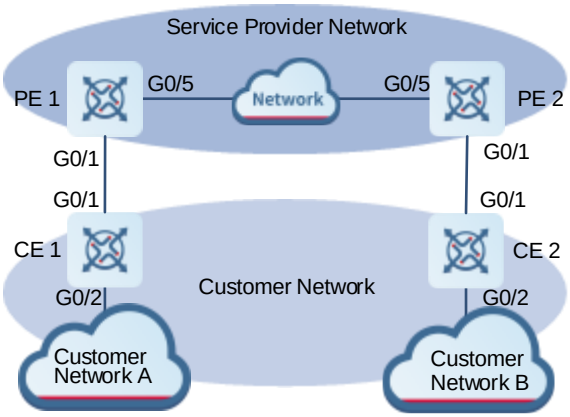
1.10.2 Configuring GVRP BPDU Tunnels

1. Requirements

As indicated in Figure 1-4, the GVRP packets of the user network are transmitted through the tunnel of the SP network.

2. Topology

Figure 1-4 Topology of GVRP BPDU Tunnels



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 GigabitEthernet 0/1 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 GigabitEthernet 0/1 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.
- Configure the basic functions of GVRP on CE 1 and CE 2, including: enabling the dynamic VLAN creation function, configuring the uplink interface Gigabit Ethernet 0/1 as the Trunk port, and enabling the GVRP function globally.

4. Procedure

(1) Configure the basic functions of GVRP on the interconnection interface of SP devices.

Enable the GVRP function globally on PE 1 and on Gigabit Ethernet 0/5 in turn. Configure static VLAN 251 to verify the GVRP function.

```
PE1> enable
PE1# configure terminal
PE1(config)# vlan 251
PE1(config-vlan)# exit
PE1(config)# gvrp dynamic-vlan-creation enable
PE1(config)# interface gigabitethernet 0/5
PE1(config-if-GigabitEthernet 0/5)# switchport
PE1(config-if-GigabitEthernet 0/5)# switchport mode trunk
PE1(config-if-GigabitEthernet 0/5)# switchport trunk native vlan 1
PE1(config-if-GigabitEthernet 0/5)# switchport trunk allowed vlan all
PE1(config-if-GigabitEthernet 0/5)# exit
PE1(config)# gvrp enable
```

Enable the GVRP function globally on PE 2 and Gigabit Ethernet 0/5 in turn. Configure static VLAN 252 to verify the GVRP function.

```
PE2> enable
PE2# configure terminal
PE2(config)# vlan 252
PE2(config-vlan)# exit
PE2(config)# gvrp dynamic-vlan-creation enable
PE2(config)# interface gigabitethernet 0/5
PE2(config-if-GigabitEthernet 0/5)# switchport
PE2(config-if-GigabitEthernet 0/5)# switchport mode trunk
PE2(config-if-GigabitEthernet 0/5)# switchport trunk native vlan 1
PE2(config-if-GigabitEthernet 0/5)# switchport trunk allowed vlan all
PE2(config-if-GigabitEthernet 0/5)# 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 0/1 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 0/1)# switchport
PE2(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE2(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 250
PE2(config-if-GigabitEthernet 0/1)# 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 0/1 of PE 2 and globally in turn.

```
PE2(config-if-GigabitEthernet 0/1)# l2protocol-tunnel gvrp enable
PE2(config-if-GigabitEthernet 0/1)# exit
PE2(config)# l2protocol-tunnel gvrp
```

(4) Configure the basic functions of GVRP on user network devices.

Enable the GVRP function globally on CE 1 and port Gigabit Ethernet 0/1 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 0/1
CE1(config-if-GigabitEthernet 0/1)# switchport
CE1(config-if-GigabitEthernet 0/1)# switchport mode trunk
CE1(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 1
CE1(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
CE1(config-if-GigabitEthernet 0/1)# exit
CE1(config)# gvrp enable
```

Enable the GVRP function globally 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)# switchport trunk native vlan 1
CE2(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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 0/5 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, Gi0/5
     251 VLAN0251                       STATIC    Gi0/5
PE1# show interface switchport
Interface             Switchport Mode     Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1     enabled    TUNNEL        250    Disabled  1,250
GigabitEthernet 0/5     enabled    TRUNK         1      Disabled  ALL
```

Only static VLANs exist on PE 2; the uplink port Gigabit Ethernet 0/5 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, Gi0/5
     252 VLAN0252                      STATIC    Gi0/5
PE2# show interface switchport
Interface            Switchport Mode     Access Native Protected VLAN lists
---------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1    enabled    TUNNEL    1      250    Disabled  1,250
GigabitEthernet 0/5    enabled    TRUNK           1      Disabled  ALL
```

Only static VLANs exist on GE 1; the unlink port Gigabit Ethernet 0/1 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    Gi0/1
CE1# show interface switchport
Interface             Switchport Mode     Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1     enabled    TRUNK          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      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 Gi0/1========
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 0/1 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 0/5          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 0/5          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 0/1          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 0/5 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, Gi0/5
     251 VLAN0251                       STATIC    Gi0/5
     252 DVLAN0252                      DYNAMIC   Gi0/5
```

Dynamic VLAN 251 has been created on PE 2, and the trunk port Gigabit Ethernet 0/5 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, Gi0/5
     251 DVLAN0251                      DYNAMIC   Gi0/5
     252 VLAN0252                       STATIC    Gi0/5
```

(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 0/1 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    Gi0/1
    70-79 DVLAN0070-DVLAN0079           DYNAMIC   Gi0/1
```

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 0/5
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- 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 dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 250
 switchport dot1q-tunnel native vlan 250
 l2protocol-tunnel gvrp enable
!
interface GigabitEthernet 0/5
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- CE 1 configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,60-69
!
interface GigabitEthernet 0/1
switchport
switchport mode trunk
switchport trunk native vlan 1
```

```
switchport trunk allowed vlan only 1-4094
```

- CE 2 configuration file

```
gvrp enable
gvrp dynamic-vlan-creation enable
!
vlan range 1,70-79
!
interface GigabitEthernet 0/1
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

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 VLAN-Mapping....5
1.1.9 MAC Address Replication....5
1.1.10 Layer-2 Protocol Tunneling....6
1.1.11 Protocols and Standards....7
1.2 Restrictions and Guidelines....7
1.3 Configuration Task Summary....8
1.3.1 Configuring Tag Adding....8
1.3.2 Configuring Tag Modification....8
1.3.3 Configuring Layer-2 Protocol Tunneling....8
1.4 Configuring Basic QinQ Encapsulation....8
1.4.1 Overview....8
1.4.2 Restrictions and Guidelines....8
1.4.3 Prerequisites....9

1.4.4 Procedure....9
1.5 Configuring C-Tag-Based Selective QinQ Encapsulation....10
1.5.1 Overview....10
1.5.2 Restrictions and Guidelines....10
1.5.3 Prerequisites....10
1.5.4 Procedure....10
1.6 Configuring ACL-Based Selective QinQ Encapsulation....11
1.6.1 Overview....11
1.6.2 Restrictions and Guidelines....11
1.6.3 Prerequisites....12
1.6.4 Procedure....12
1.7 Configuring MAC Address Replication....13
1.7.1 Overview....13
1.7.2 Restrictions and Guidelines....13
1.7.3 Prerequisites....14
1.7.4 Procedure....14
1.8 Configuring Priority Replication or Priority Mapping....15
1.8.1 Overview....15
1.8.2 Restrictions and Guidelines....15
1.8.3 Configuration Tasks....15
1.8.4 Configuring Priority Replication....16
1.8.5 Configuring Priority Mapping....16
1.9 Configuring TPID....17
1.9.1 Overview....17

1.9.2 Restrictions and Guidelines 18
1.9.3 Prerequisites 18
1.9.4 Procedure 18
1.10 Configuring QinQ Tag Modification Policy 19
1.10.1 Overview 19
1.10.2 Restrictions and Guidelines 19
1.10.3 Prerequisites 20
1.10.4 Procedure 20
1.11 Configuring VLAN-Mapping 21
1.11.1 Overview 21
1.11.2 Restrictions and Guidelines 22
1.11.3 Prerequisites 22
1.11.4 Procedure 22
1.12 Configuring Layer-2 Protocol Tunneling 23
1.12.1 Overview 23
1.12.2 Restrictions and Guidelines 23
1.12.3 Configuration Tasks 23
1.12.4 Configuring STP Packet Tunneling 24
1.12.5 Configuring GVRP Packet Tunneling 25
1.13 Monitoring 25
1.14 Configuration Examples 27
1.14.1 Configuring Basic QinQ to Implement Layer-2 VPN 27
1.14.2 Configuring C-Tag-Based Selective QinQ to Implement Layer-2 VPN and Service Flow Management 35

1.14.3 Configuring ACL-Based Selective QinQ to Implementing Layer-2 VPN and Service Flow Management 40

1.14.4 Configuring VLAN-Mapping to Implement Aggregation of Different Services 43

1.14.5 Configuring Layer-2 Protocol Tunneling Based on QinQ 52

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

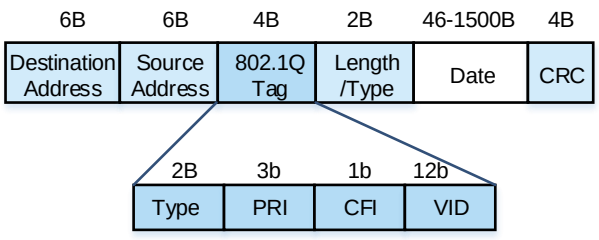
- QinQ is a kind of dual-tag encapsulation technology. It adds outer VLAN tags to packets in the SP network so that client VLANs in different private networks can be reused to increase the number of VLAN tags available to clients. The number of VLANs actually available to SPs is increased to 4094x4094.
- 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

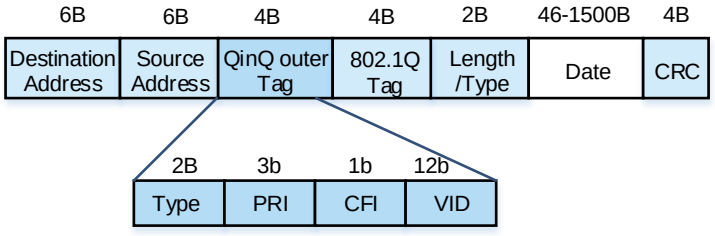


- **Type**: Consisting of 2 bytes; 0x8100 indicates 802.1Q frame. Devices that do not support IEEE 802.1Q will drop such frames received.
- **PRI**: Consisting of 3 bits, indicating layer-2 priority. The value range is 0 to 7, corresponding to CoS priorities of QoS. A larger value indicates a higher 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. 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 dot1q-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.

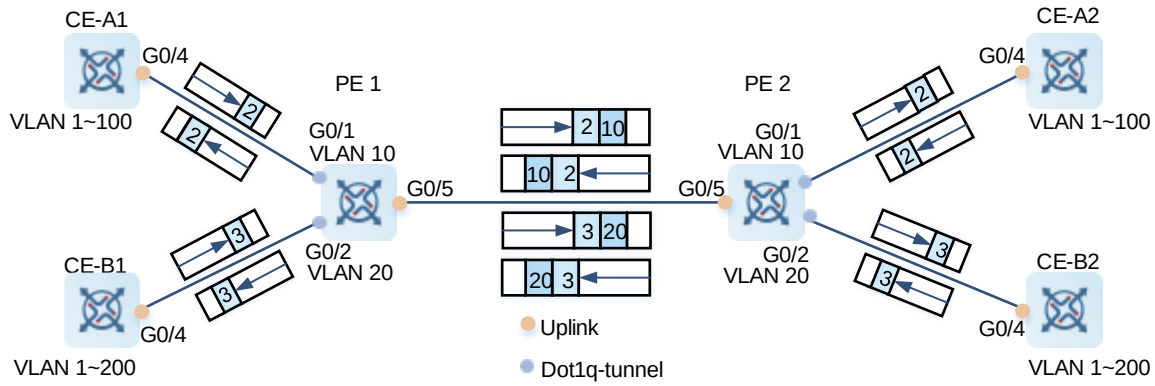
2. QinQ Forwarding

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 dot1q-tunnel port with native VLAN set to VLAN 10. The dot1q-tunnel port then strips the outer tag of the packet and sends the packet to CE-A2. This process is called QinQ decapsulation. 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

In the QinQ scenario, the PE edge port connected to the client network will first encapsulate the outer tag for the user packets, and then transmit the packets in the ISP network. The edge port must be configured as a dot1q tunnel port. One dot1q tunnel port can have one native VLAN and several allowed VLANs. Allowed VLANs are divided into Tagged VLANs and Untagged VLANs. The dot1q tunnel port can only be connected to trunk links.

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. Therefore, the VLAN of the ISP network must be configured as the native VLAN of the dot1q tunnel port. To ensure the communication of upstream and downstream packets, the native VLAN must be added to the allowed untagged VLAN list of the 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 packet content 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.

To solve this problem, use the function in MAC Address Replication to replicate the MAC address of the native VLAN to the outer VLAN.

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 VLAN-Mapping

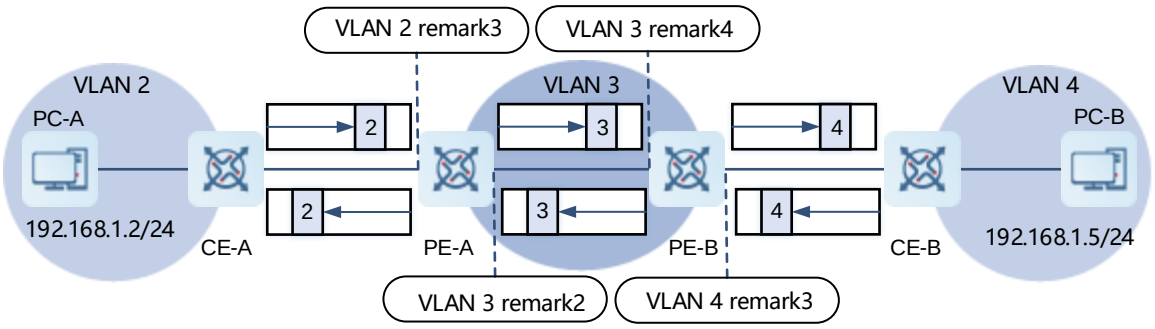
The VLAN mapping function can convert client VLAN IDs and SP VLAN IDs to implement inter-VLAN layer-2 communication. This function takes effect on the access, trunk, hybrid, or uplink ports. VLAN mapping is a function of modifying tags, not adding tags.

As shown in Figure 1-4, when receiving a client packet of PC-A in VLAN 2, PE-A replaces private VLAN 2 in the packet with public VLAN 3 for transmission according to the configured mapping relationship VLAN 2 remark 3; when receiving a packet from public VLAN 3, PE-B maps public VLAN 3 to client VLAN 4 according to the mapping relationship VLAN 3 remark 4 so that PC-B can receive the packet. When receiving a client packet of PC-B in VLAN 4, PE-B restores private VLAN 4 in the packet to public VLAN 3 for transmission according to the mapping relationship VLAN 4 remark 3; when receiving a packet from public VLAN 3, PE-A restores public VLAN 3 to client VLAN 2 according to the mapping relationship VLAN 3 remark 2 so that PC-A can receive the response packet. In this way, inter-VLAN layer-2 communication is achieved between PC-A and PC-B.

If the planning of two client networks is asymmetric or the VLAN IDs of the new and old networks conflict with each other, the VLAN mapping function can be used to achieve inter-VLAN layer-2 communication. Two prerequisites are required for this communication mode:

- The clients at two ends are in the same network segment. If the receiving and sending end clients are not in the same network segment, they will rely on layer-3 communication, and VLAN mapping makes no sense.
- The packet received by PE needs to carry a tag. Therefore, the uplink port of CE needs to send the packet carrying a tag.

Figure 1-4 Introduction to the VLAN Mapping Function



1.1.9 MAC Address Replication

- Source

After receiving a packet, the interface will learn the corresponding relationship between the source MAC address of the packet and the VLAN and write it to the MAC address table. If receiving a tagged packet, the access, trunk, hybrid, and uplink ports will learn the corresponding relationship between the VLAN ID and MAC address in the tag; if receiving an untagged packet, they will learn the corresponding relationship between the native VLAN and MAC address. After receiving packets, the dot1q-tunnel port regards all the packets as untagged regardless of whether they carry tags, and determines whether the packets belong to the native VLAN of the local interface. Therefore, the dot1q-tunnel port always learns the corresponding relationship between its native VLAN and client MAC address.

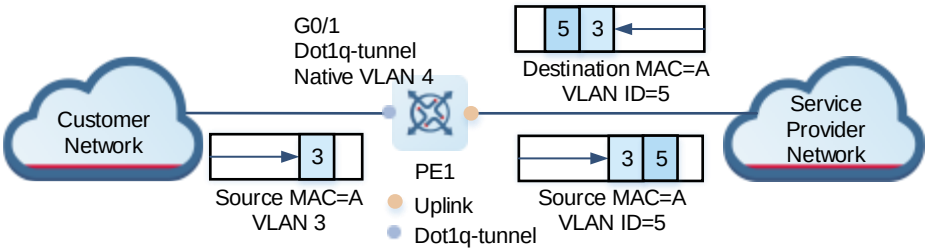
If basic QinQ encapsulation is used, the VLAN ID in the outer tag is native VLAN ID. When receiving a response packet from the peer end, the device can find the corresponding relationship between the client MAC address and the outer VLAN in the MAC address table. If selective QinQ encapsulation is used, the VLAN ID in the outer tag is not the native VLAN ID. When receiving a response packet from the peer end, the device cannot find the matched MAC address entry, and therefore it will perform packet flooding, occupying network resources and affecting the performance.

If the MAC address replication function is enabled, when learning a dynamic address, the interface can replicate the MAC address in the native VLAN to the VLAN where the outer tag is located, thus solving the problem of continuous flooding of the packets returned from the public network. Similarly, the MAC address in the VLAN where the outer tag is can also be replicated to the native VLAN to avoid continuous flooding of the packets from the client network to the public network.

- Principles

As shown in Figure 1-5, the interface connecting PE 1 and the client network is dot1q-tunnel, and native VLAN 4 is configured on this interface. Configure an ACL-based QinQ encapsulation policy, and encapsulate the packet with source MAC address A by using the outer tag VLAN 5. When receiving a packet of client network VLAN 3 and source MAC address A from the interface Gigabit Ethernet 0/1, PE 1 adds the outer tag of VLAN 5. At the same time, because the native VLAN of the receiving interface is VLAN 4, PE1 learns the entry <VLAN 4, MAC-A, GigabitEthernet 0/1>. When a response packet is returned, because the VLAN ID of its outer tag is 5, PE 1 will look for MAC-A in VLAN 5, but MAC-A is not learned into VLAN 5, and therefore this packet will be flooded. If MAC address replication is configured and MAC-A in VLAN 4 is replicated to VLAN 5, the dynamic MAC address entry <VLAN 5, MAC-A, GigabitEthernet 0/1> will be added to PE 1. When a response packet is returned, PE 1 can find that the packet should be forwarded to GigabitEthernet 0/1, thus avoiding flooding.

Figure 1-5 MAC Address Replication



1.1.10 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, 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, the STP and GVRP packets of the client network must be transmitted 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.

1.1.11 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

- The QinQ feature only takes effect on a Layer 2 interface. A Layer 3 interface cannot be directly configured as a dot1q tunnel port, and must be configured as a Layer 2 interface first.
- You can use the **show interface switchport** command to view the interface type. If the Switchport field corresponding to the interface is "enabled", it means that the interface is a Layer 2 interface. If the Switchport field corresponding to the interface is "disabled", it means that the interface is a Layer 3 interface.
- You can use the **switchport** command to configure the interface as a Layer 2 interface. First, use the **no switchport mode** command to restore the mode of the Layer 2 interface to the default value, and then use the **no switchport** command to configure the Layer 2 interface as a Layer 3 interface. When the Layer 2/Layer 3 mode of the interface is modified, all properties of the interface are restored to the default values of the interface type.
- The IEEE 802.1x function cannot be enabled on an interface configured as a dot1q-tunnel port.
- The port security function cannot be enabled on an interface configured as a dot1q-tunnel port.
- When a dot1q-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 dot1q-tunnel port with the VID in the client tag, use the **inner** keyword. See *Configuring ACL* in *ACL and QoS Configuration Guide*.
- You are advised to 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 dot1q-tunnel port. Select at least one of them to configure.

- Configuring Basic QinQ Encapsulation
- Configuring C-Tag-Based Selective QinQ Encapsulation
- Configuring ACL-Based Selective QinQ Encapsulation

(2) (Optional) Configuring MAC Address Replication

(3) (Optional) Configuring Priority Replication or Priority Mapping. The following configuration tasks are mutually exclusive.

- Configuring Priority Replication
- Configuring Priority Mapping

(4) (Optional)Configuring TPID

1.3.2 Configuring Tag Modification

Configure the tag modification mode. The following tasks are optional.

- Configuring QinQ Tag Modification Policy.
- Configuring VLAN-Mapping

1.3.3 Configuring Layer-2 Protocol Tunneling

Configuring Layer-2 Protocol Tunneling includes the following tasks:

- 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 Prerequisites

- Configure the interface as a Layer 2 interface.

1.4.4 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) Enter the interface configuration mode, and configure the interface for connecting to the client network.

a Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

o Enter the Layer 2 aggregate interface configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

b Configure the Layer 2 interface 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 a Layer 2 aggregate interface, the policy of adding or modifying the VID configured on the aggregate interface is deleted and needs to be reconfigured. You are advised to configure the VIP policy on an aggregate interface after configuring the members.
- You must configure the dot1q-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 Prerequisites

Configure the interface as a Layer 2 interface.

1.5.4 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) Enter the interface configuration mode to configure the interface for connecting the client network.

- Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the Layer 2 Ethernet interface as a dot1q-tunnel port.

switchport mode dot1q-tunnel

A Layer 2 interface works in access mode by default.

(4) 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.

(5) 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 ACL-Based Selective QinQ Encapsulation

1.6.1 Overview

Encapsulate outer VLAN tags (S-Tags) in packets based on the ACL-based flow classification to allow the SP network to manage different services.

For input packets of dot1q-tunnel port on the network, if the outer tags with different VLAN IDs need to be added according to different packet contents, this function must be configured.

1.6.2 Restrictions and Guidelines

- 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.
- The **expert access-list extended** command is used to configure the extended expert ACL and enter the extended expert ACL configuration mode. The command format is as follows: **expert access-list extended** { *acl-name* | *acl-number* }. *acl-name*: Extended expert ACL name. The value is a case-sensitive string of 1 to 99 characters. *acl-number*: Extended expert ACL number. The value range is from 2700 to 2899. For the sake of easy description, the **expert access-list extended** *acl-number* command is taken as an example in the configuration procedure.

  The **permit** command is used to add an ACL rule of the allowed type to an ACL. For the detailed syntax, see *Configuring ACL*. For the sake of easy description, the **permit** *ethernet-type any any* command is taken as an example in the configuration procedure.

Caution

- The policy of adding the VID based on ACL prevails over those based on C-Tag and port.
- When an ACL is deleted, the related policy will be automatically deleted.
- Upon receiving a packet with two or more tags, the dot1q-tunnel port cannot add an outer tag to the packet based on the flow-based matching rule.
- If a packet matches two or more data flow-based VID adding policies without priority, only one policy is executed. You are advised to specify the priority when configuring a policy.
- You must configure the dot1q-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.

1.6.3 Prerequisites

Configure the interface as a Layer 2 interface.

1.6.4 Procedure

(1) Create a traffic classification and define a packet matching rule.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a professional extended ACL *acl-number-a* and enter the professional extended ACL configuration mode.

expert access-list extended *acl-number-a*

By default, there is no professional extended ACL rule in the ACL.

d Add an ACL rule of the allowed type to ACL *acl-number-a*.

permit *ethernet-type-a any any*

By default, there is no ACL rule of the allowed type in the ACL.

e Return to the global configuration mode.

exit

f Create a professional extended ACL *acl-number-b* and enter the professional extended ACL configuration mode.

expert access-list extended *acl-number-b*

By default, there is no professional extended ACL rule in the ACL.

g Add an ACL rule of the allowed type to ACL *acl-number-b*.

permit *ethernet-type-b any any*

By default, there is no ACL rule of the allowed type in the ACL.

h Return to the global configuration mode.

exit

(2) Create an SP VLAN.

a Create a group of SP VLANs.

vlan range *svidA,svidB*

Only VLAN 1 exists by default.

b Return to the global configuration mode.

exit

(3) Enter the interface configuration mode to configure the interface for connecting the client network.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the Layer 2 Ethernet interface as a dot1q-tunnel port.

switchport mode dot1q-tunnel

A Layer 2 interface works in access mode by default.

(5) 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.

(6) Configure the ACL-based QinQ encapsulation rule. The packets matching different ACL rules are allocated to different SP VLANs for transmission through a tunnel.

a The packets matching ACL *acl-number-a* are allocated to the SP VLAN *svidA*.

traffic-redirect access-group *acl-number-a* **nested-vlan** *svidA* **in**

The policy of adding an outer VLAN ID based on ACL is not configured by default.

b The packets matching ACL *acl-number-b* are allocated to the SP VLAN *svidB*.

traffic-redirect access-group *acl-number-b* **nested-vlan** *svidB* **in**

The policy of adding an outer VLAN ID based on ACL is not configured by default.

1.7 Configuring MAC Address Replication

1.7.1 Overview

If selective QinQ encapsulation is used, the VLAN ID in the outer tag is not the native VLAN ID. When receiving a response packet from the peer end, the device cannot find the matched MAC address entry, and therefore it will perform packet flooding, occupying network resources and affecting the performance.

If the MAC address replication function is enabled, when learning a dynamic address, the dot1q-tunnel port can replicate the MAC address in the native VLAN to the VLAN where the outer tag is located, thus solving the problem of continuous flooding of the packets returned from the public network. Similarly, the MAC address in the VLAN where the outer tag is can also be replicated to the native VLAN to avoid continuous flooding of the packets from the client network to the public network.

1.7.2 Restrictions and Guidelines

- The MAC address replication function cannot be configured on the host and promiscuous interfaces, or the destination interface with port security and imaging enabled, or the interface with the 802.1x function

enabled.

- After MAC address replication is disabled, the system will delete all the learned MAC address entries from the destination VLAN. The MAC address entries obtained through MAC address replication between VLANs cannot be deleted manually. When you need to delete these entries, disable MAC address replication.
- *mapping-id* indicates the index number of the MAC address replication policy. The value range is from 1 to 8, and therefore each port can be configured with up to eight destination VLANs.
- *source-vlan-list* indicates the source VLAN list. The value range is from 1 to 4094. One single command can contain one or more VLANs.
- *destination-vlan-id* indicates the destination VLAN. The value range is from 1 to 4094. Only one destination VLAN can be specified in one command. MAC address replication between VLANs can be configured on an interface for one single destination VLAN once only. To make modification, you need to delete the previous configuration before reconfiguration. MAC address replication takes effect even if the interface does not belong to the specified destination VLAN. MAC address replication does not support address replication to dynamic VLANs.
- MAC address replication replicates only dynamic addresses. Address replication is disabled when the address table is full. If source addresses already exist before replication is enabled, corresponding MAC addresses will not be replicated. Replicated addresses have a higher priority than dynamic addresses but have a lower priority than other types of addresses.
- When a MAC address ages, the replicated MAC address will also age. When the MAC address is deleted, the replicated address will be deleted automatically.
- This function does not support hot backup. After primary/secondary switchover occurs, you are advised to disable MAC address replication and then enable it again.

1.7.3 Prerequisites

Configure the interface as a Layer 2 interface.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(4) Configure the MAC address replication policy, and enable the MAC address replication function.

mac-address-mapping *mapping-id* **source-vlan** *source-vlan-list* **destination-vlan** *destination-vlan-id*

The MAC address replication function is disabled by default.

1.8 Configuring Priority Replication or Priority Mapping

1.8.1 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.

1.8.2 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.
- The order of priority effectiveness from high to low is: priority mapping, QoS based on ACL data flow, priority replication, and QoS based in trust mode.
- If the interface trust mode is not configured (i.e. interface Trust None), the priority mapping will not take effect. If the configured trust mode does not match the configured mapping rule, priority mapping will also not take effect.

1.8.3 Configuration Tasks

The following configuration tasks are mutually exclusive. Select one task.

- Configuring Priority Replication
- Configuring Priority Mapping

1.8.4 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. Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the Layer 2 interface as a dot1q tunnel port.
- Configure the QinQ encapsulation mode of the dot1q tunnel port.

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 Layer 2 Ethernet interface configuration mode

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(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.

1.8.5 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

- The value range of *inner-cos-value* and *outer-cos-value* are from 0 to 7.

- If priority mapping is not configured, the mapping rules shown in Table 1-1 are used by default.

Table 1-1 Default Priority Mapping

inner-cos-value	0	1	2	3	4	5	6	7
outer-cos-value	0	1	2	3	4	5	6	7

3. Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the Layer 2 interface as a dot1q tunnel port.
- Configure the QinQ encapsulation mode of the dot1q tunnel port.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(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.

1.9 Configuring TPID

1.9.1 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.

1.9.2 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.

1.9.3 Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the interface as an Uplink port.

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, and configure the uplink port (the port where the SP's network edge device connects to the public network).

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the TPID value.

frame-tag tpid *tpid*

The TPID value is 0x8100 by default.

1.10 Configuring QinQ Tag Modification Policy

1.10.1 Overview

Packets encapsulated by QinQ carries double tags, and must be transmitted in the SP network. The Access, Trunk, Hybrid and Uplink ports of the device can receive and forward packets carrying double tags, while the dot1q tunnel port will discard packets carrying double tags.

In the SP network, the outer tag or inner tag of data packets of the SP network may need to be modified due to the actual networking topology requirements. In this case, the QinQ tag modifying function needs to be used. The device supports the following modification policies:

- Modify the outer VID based on the outer VID of packet

  For inbound packets on access, trunk, hybrid and uplink ports, this function can modify the VID of the outer tag to a different VID value according to the different VID in the inner tag of the packet.

- Modify the outer VID based on the inner VID of packet

  For inbound packets on access, trunk, hybrid and uplink ports, this function can modify the VID of the outer tag according to the inner and outer VID of the packet before the packet is forwarded.

- Modify the outer VID based on the outer and inner VIDs of packet

  For the inbound packets on access, trunk, hybrid and uplink ports, this function can modify the VID of the outer tag according to the VID in the outer tag of the packet before the packet is forwarded.

- Modify the outer VID based on the content of packet

  For the outbound packets on access, trunk, hybrid and uplink ports, this function can modify the VID of the inner tag based on the packet content identified by ACL.

- Modify the inner VID based on the content of packet

  For the outbound packets on access, trunk, hybrid and uplink ports, this function can modify the VID of the outer tag based on the packet content identified by ACL.

1.10.2 Restrictions and Guidelines

- The policy of modifying the VID based on ACL prevails over those based on port and C-Tag.
- The function of modifying VID according to packet content requires configuring ACL to distinguish data flow. When an ACL is deleted, the related policy will be automatically deleted.
- The modification policy takes effect only on the access, trunk, hybrid, and uplink ports.
- If a packet matches two or more VID modification policies without priority, only one policy is executed.
- *new-svid* indicates the VID of the outer tag after modification, *old-svid* indicates the VID of the outer tag before modification, *old-svid-list* indicates the VID list of the outer tag before modification, which are VLAN IDs of the SP network.
- *cvid-list* indicates the VID list of the inner tag after modification, *new-cvid* indicates the VID of the inner tag after modification, which are VLAN IDs of the client network.
- *acl-name* indicates the name of the ACL policy for matching data flow. The value is a case-sensitive string of 1-99 characters. *acl-number* indicates the number of the ACL policy for matching data flow. The value range of IP standard ACL is 1-99 and 1300-1999. The value range of IP extended ACL is 100-199 and 2000-2699. The value range of MAC standard ACL is 700-799. The value range of extended expert ACL is 2700-2899.

See *Configuring ACL* in *ACL and QoS Configuration Guide*.

1.10.3 Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the Layer 2 interface as an access, trunk, hybrid or uplink port.

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.

- Enter the Layer 2 Ethernet interface configuration mode

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the tag modification policy of double-tagged inbound packets. Please select at least one of them to configure.

- Configure the policy of modifying the outer VID based on the inner VID of packet.

dot1q relay-vid *new-svid* **translate inner-vid** *cvid-list*

No policy of modifying the outer VID based on the inner VID of packets is configured by default.

- Configure the policy of modifying the outer VID based on the outer VID of the packet.

dot1q relay-vid *new-svid* **translate local-vid** *old-svid-list*

No policy of modifying the outer VID based on the outer VID of input packets is configured by default.

- Configure the policy of modifying the outer VID based on the outer and inner VIDs of packet.

dot1q new-outer-vlan *new-svid* **translate old-outer-vlan** *old-svid* **inner-vlan** *cvid-list*

No policy of modifying the outer VID based on the outer and inner VIDs of packet is configured by default.

(5) Configure the tag modification policy of double-tagged outbound packets. Please select at least one of them to configure.

- Configure the policy of modifying the inner VID based on the packet content.

traffic-redirect access-group { *acl-name* | *acl-number* } **inner-vlan** *new-cvid* **out**

No policy of modifying the inner VID based on packet content is configured by default.

- Configure the policy of modifying the outer VID based on the packet content.

traffic-redirect access-group { *acl-name* | *acl-number* } **outer-vlan** *new-svid* **in**

No policy of modifying the outer VID based on the packet content is configured by default.

1.11 Configuring VLAN-Mapping

1.11.1 Overview

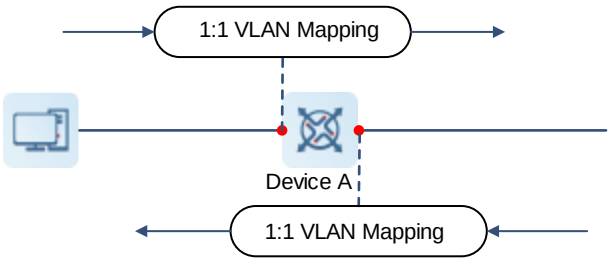
The function is used to replace the VLAN ID of a packet of the client network with a public VLAN ID so that the packet can be transmitted according to the VLAN rules of the public network; or replace the VLAN ID of a packet of the public network with a VLAN ID of the client network so that the packet can be transmitted according to VLAN planning of the client network.

- 1:1 VLAN Mapping In

On the input interface of a device, the VID of the packet on one VLAN is modified to a VID of another VLAN. This mapping method is called one-to-one VLAN mapping in the input direction. This function is used for floor devices to use different VLANs to carry the same service from different clients and differentiate clients.

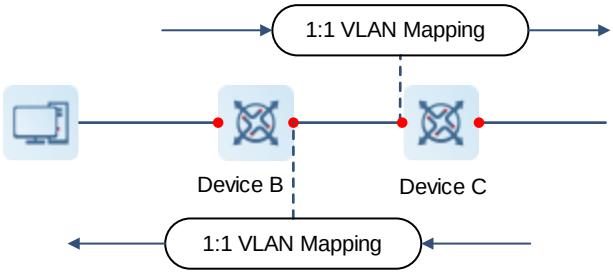
As shown in Figure 1-6, VLAN mapping in the input direction is configured on a single device (Device A). For uplink data flow, the VLAN mapping policy in the input direction is configured on the downlink port, and the original VLAN ID is mapped to a new VLAN ID before packet output from the uplink port. For downlink data flow, the VLAN mapping policy in the input direction is configured on the uplink port, and the packet VLAN ID is mapped to the original VLAN ID before packet output from the downlink port.

Figure 1-6 Configuring 1:1 VLAN Mapping in Input Direction on Single Device



As shown in Figure 1-7, VLAN mapping in the input direction is configured on two devices (Device B and Device C). For uplink data flow, the VLAN mapping policy in the input direction is configured on the downlink port of Device C, and the original VLAN ID is mapped to a new VLAN ID before packet output from the uplink port. For downlink data flow, the VLAN mapping policy in the input direction is configured on the uplink port of Device B, and the packet VLAN ID is mapped to the original VLAN ID before packet output from the downlink port.

Figure 1-7 Configuring 1:1 VLAN Mapping in Input Direction on Two Devices



1.11.2 Restrictions and Guidelines

- 1:1 VLAN Mapping In:

  For uplink data flow, the source VLAN is a client VLAN; the destination VLAN is an SP VLAN.

  For downlink data flow, the source VLAN is an SP VLAN; the destination VLAN is a client VLAN.

- When the VLAN mapping function in input direction is enabled, the VLAN ID of the packet sent to the CPU is the VLAN ID after modification. The interface only needs to allow the VLAN after modification to pass. If the VLAN data before modification does not need to be forwarded on the device, you do not need to create a VLAN before modification on the device.
- The VLAN tags of public network packets whose destination MAC address is multicast, broadcast, or unknown unicast address cannot be replaced with the VLAN tag of the client private network.
- VLAN mapping can be configured only on the access, trunk, hybrid, or uplink port. Do not configure VLAN mapping and selective QinQ on the same interface.
- The interface configured with VLAN mapping must be added to the mapped VLAN.

1.11.3 Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the Layer 2 interface as an Access, Trunk, Hybrid or Uplink port.

1.11.4 Procedure

(1) Create a VLAN after mapping.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create a VLAN after mapping.

vlan *destinationdest-vlan-id*

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the VLAN mapping policy in the inbound direction on the interface.

vlan-mapping-in vlan *source-vlan-id* **remark** *destination-vlan-id* [**in-only**]

No VLAN mapping policy in the inbound direction is configured by default.

Note

This section describes only the procedure of configuring one mapping policy on an interface, without reflecting the mapping logic. The mapping relationship needs to be configured on multiple interfaces to reflect the mapping logic.

1.12 Configuring Layer-2 Protocol Tunneling

1.12.1 Overview

BPDU tunneling is a layer-2 tunneling function based on the Layer 2 Tunnel Protocol (L2TP).

Spanning tree protocol packets use the dedicated multicast address 0180.c200.0000 as the destination MAC address. GVRP protocol packets use the dedicated multicast address 0180.c200.0006 as the destination MAC address. When the dot1q-tunnel port of the SP edge device receives these two types of packets, it will not treat them as ordinary client packets. The edge device will identify them as BPDU packets and will not forward them. The spanning tree calculation is performed according to the contents of the spanning tree BPDU, and VLAN information will be updated according to GVRP protocol packets by adding or deleting VLANs, which 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 protocol packets on the client network enter the dot1q-tunnel 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 protocol packets through the tunnel in the SP network, preventing the client network and the SP network from interfering with each other.

1.12.2 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 dot1q-tunnel 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.

1.12.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring STP Packet Tunneling
- Configuring GVRP Packet Tunneling

1.12.4 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.

- When the spanning tree protocol packets in the client network enters the dot1q tunnel port of the edge device, its destination MAC address is changed from the public address 0180.c200.0000 to the private address (default is 01d0. f800.0005) before forwarding the packets in the SP network.
- After packets are forwarded to the edge device at the other end, the destination MAC address is changed from the private address (the default is 01d0. f800.0005) to the public address 0180.c200.0000 before and transmitting the packets in the client network at the other end.

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. Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the Layer 2 interface as a dot1q tunnel port.

4. 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.

- Enter the Layer 2 Ethernet interface configuration mode
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(6) Enable STP packet tunnelling function on the dot1q-tunnel port.
l2protocol-tunnel stp enable

The STP packet tunneling function is disabled on the dot1q-tunnel port by default.

1.12.5 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.

- When the spanning tree protocol packets in the client network enters the dot1q tunnel port of the edge device, its destination MAC address is changed from the public address 0180.c200.0000 to the private address (default is 01d0. f800.0006) before forwarding the packets in the SP network.
- After packets are forwarded to the edge device at the other end, the destination MAC address is changed from the private address (the default is 01d0. f800.0006) to the public address 0180.c200.0000 before and transmitting the packets in the client network at the other end.

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. Prerequisites

- Configure the interface as a Layer 2 interface.
- Configure the Layer 2 interface as a dot1q tunnel port.

4. 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.

- Enter the Layer 2 Ethernet interface configuration mode
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(6) Enable GVRP packet tunneling function on dot1q-tunnel port.
l2protocol-tunnel gvrp enable

The GVRP packet tunneling function is disabled for the dot1q-tunnel port by default.

1.13 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.
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 interfaces [*interface-type interface-number*] **vlan-mapping**	Displays the VLAN mapping policy on the interface.
show traffic-redirect [**interfaces** *interface-type interface-number*]	Displays the policy of modifying or adding the VID based on data flow.
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 interfaces mac-address-mapping	Displays the configuration of MAC address replication.
show l2protocol-tunnel { **gvrp** | **stp** }	Displays the layer-2 tunnel configuration.
debug bridge qinq	Enables the QinQ debugging function.

1.14 Configuration Examples

1.14.1 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 1-8. 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 dot1q-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 dot1q-tunnel 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.

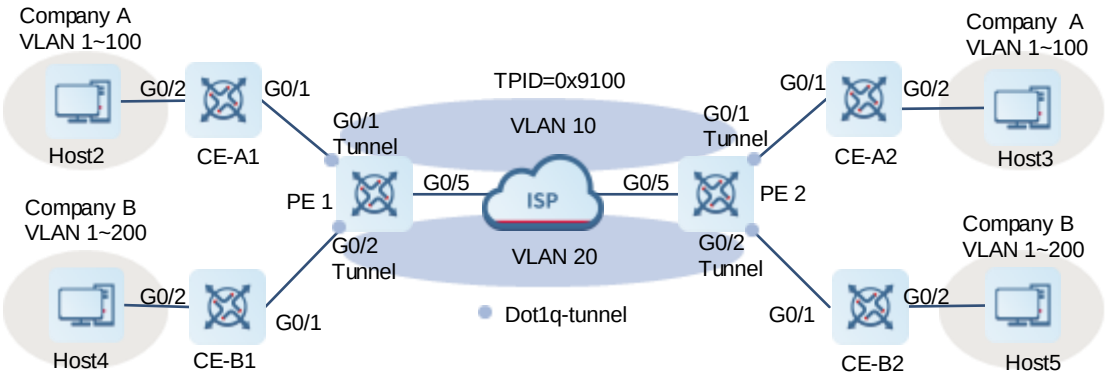
- The office network VLAN of Company A ranges from 1 to 100.
- The office network VLAN of Company B ranges from 1 to 200.

The priority replication and priority mapping functions of CoS can be configured on the dot1q-tunnel 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 1-8 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 dot1q-tunnels.

The public network transmission VLAN is the native VLAN of the dot1q-tunnel, 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 dot1q-tunnel, and belongs to the allowed untagged VLAN list of the dot1q-tunnel.

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 dot1q-tunnel, and belongs to the allowed untagged VLAN list of the dot1q-tunnel.

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
PE1(config-if-GigabitEthernet 0/5)# switchport mode trunk
PE1(config-if-GigabitEthernet 0/5)# switchport trunk native vlan 1
PE1(config-if-GigabitEthernet 0/5)# switchport trunk allowed vlan all
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
PE2(config-if-GigabitEthernet 0/5)# switchport mode trunk
PE2(config-if-GigabitEthernet 0/5)# switchport trunk native vlan 1
PE2(config-if-GigabitEthernet 0/5)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
CE-A1(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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 mode access
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)# switchport trunk native vlan 1
CE-A2(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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 mode access
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)# switchport trunk native vlan 1
CE-B1(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
CE-B2(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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        10     Disabled  1,10
GigabitEthernet 0/2           enabled    TUNNEL        20     Disabled  1,20
GigabitEthernet 0/5           enabled    TRUNK         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        10     Disabled  1,10
GigabitEthernet 0/2           enabled    TUNNEL        20     Disabled  1,20
GigabitEthernet 0/5           enabled    TRUNK         1      Disabled  ALL
```

(2) Display the dot1q-tunnel configuration of PEs.

Display the dot1q-tunnel 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 dot1q-tunnel 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
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
!
interface GigabitEthernet 0/2
switchport
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 20
 switchport dot1q-tunnel native vlan 20
!
interface GigabitEthernet 0/5
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094 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
switchportswitchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
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
switchport mode trunk
```

```
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface gigabitethernet 0/2
switchport
 switchport mode accessswitchport 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.

1.14.2 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 dot1q-tunnel; the basic QinQ cannot meet the requirement for differentiating SP VLANs in multi-service scenarios.

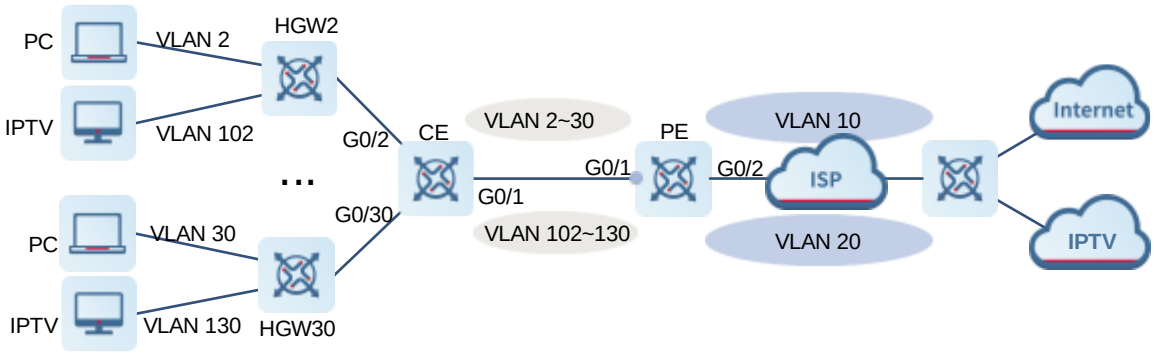
Selective QinQ can flexibly add the SP outer tag (S-Tag) according to the tag (C-Tag) of client packets, encapsulate the client service flows received by the same dot1q-tunnel into different SP VLANs, and use the QoS policy of SP network to guarantee reliability while transparently transmitting client data.

As shown in Figure 1-9, 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 dot1q-tunnel 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 1-9 Configuring C-Tag-based Selective QinQ to Implement Layer-2 VPN and Service Flow Management



3. Notes

- Configure the interface GigabitEthernet 0/1 of PE for connecting to CE as dot1q-tunnel. Add SP VLANs 10 and 20 to the untagged VLAN list of the dot1q-tunnel connected to the client network so that the packets from the peer end return to the dot1q-tunnel 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 dot1q-tunnel 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 dot1q-tunnel 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 dot1q-tunnel 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 native vlan 1
PE(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 1,10,20
```

If the dot1q-tunnel 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 dot1q-tunnel 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 dot1q-tunnel, 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
PE(config-if-GigabitEthernet 0/2)# switchport mode uplink
PE(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
PE(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
CE(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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 native vlan 1
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 native vlan 1
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     Disabled  1,10,20
GigabitEthernet 0/2            enabled    UPLINK        1     Disabled  ALL
```

Display the dot1q-tunnel 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     Disabled  ALL
GigabitEthernet 0/2           enabled   Trunk         1     Disabled  2,102
GigabitEthernet 0/3           enabled   Trunk         1     Disabled  3,103
……
GigabitEthernet 0/30          enabled   Trunk         1     Disabled  30,130
```

6. Configuration Files

- Configuration file of the PE

```
vlan range 1,10,20
!
interface GigabitEthernet 0/1
switchport
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 1, 10,20
switchport dot1q-tunnel native vlan 1
 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
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- 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
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 2,102
!
interface GigabitEthernet 0/30
 switchport
switchport mode trunk
switchport trunk native vlan 1switchport trunk allowed vlan only 30,130
```

1.14.3 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 1-10, 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.

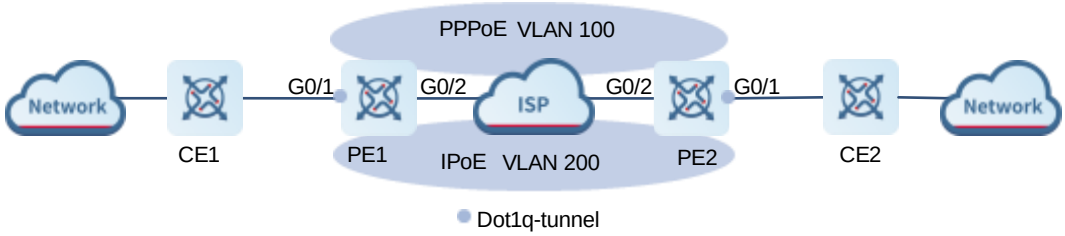
The selective QinQ function based on ACL is used on PE 1 and PE 2 to encapsulate different service data of the company with different outer VLAN tags so that the data can be transmitted through the SP network transparently and the branches can access each other's network.

- 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 1-10 Configuring ACL-based Selective QinQ to Implement Layer-2 VPN and Service Flow Management



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 dot1q-tunnel, 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 dot1q-tunnel.

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 dot1q-tunnel 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
PE1(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 1
PE1(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 1,100,200
```

If the dot1q-tunnel receives frames matching ACL1, the frames will be encapsulated with the tag of SP VLAN 100.

```
PE1(config-if-GigabitEthernet 0/1)# traffic-redirect access-group acl1
nested-vlan 100 in
```

If the dot1q-tunnel receives frames matching ACL2, the frames will be encapsulated with the tag of SP VLAN 200.

```
PE1(config-if-GigabitEthernet 0/1)# traffic-redirect access-group acl2
nested-vlan 200 in
```

Configure the MAC address replication function to replicate the learned MAC address from the default native VLAN 1 of the dot1q-tunnel to VLAN 100 of outer tag.

```
PE1(config-if-GigabitEthernet 0/1)# mac-address-mapping 1 source-vlan 1
destination-vlan 100
```

(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)# switchportPE1(config-if-GigabitEthernet
0/2)# switchport mode uplink
PE1(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
PE1(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan
allPE1(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     Disabled
1,100,200
GigabitEthernet 0/2            enabled    UPLINK         1     Disabled  ALL
```

(2) Verify the encapsulation policy for adding tags based ACL.

```
PE1# show traffic-redirect
Ports      Type        VID    Match-filter
-------    ----------    -----   ------------
Gi0/1      Nested-vid   100       acl1
Gi0/1      Nested-vid   200       acl2
```

(3) Display the priority mapping relationship on the interface.

```
PE1# show interfaces gigabitethernet 0/1 remark
Ports       From COS  To COS
------------ --------- --------
Gi0/1       3       5
```

(4) 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
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 1,100,200
switchport dot1q-tunnel native vlan 1
dot1q-tunnel cos 3 remark-cos 5
traffic-redirect access-group acl1 nested-vlan 100 in
 traffic-redirect access-group acl2 nested-vlan 200 in
mls qos trust cos
!
interface GigabitEthernet 0/2
 switchport
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

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.
- The MAC address replication function is not configured, which may lead to packet flooding.

1.14.4 Configuring VLAN-Mapping to Implement Aggregation of Different Services

1. Requirements

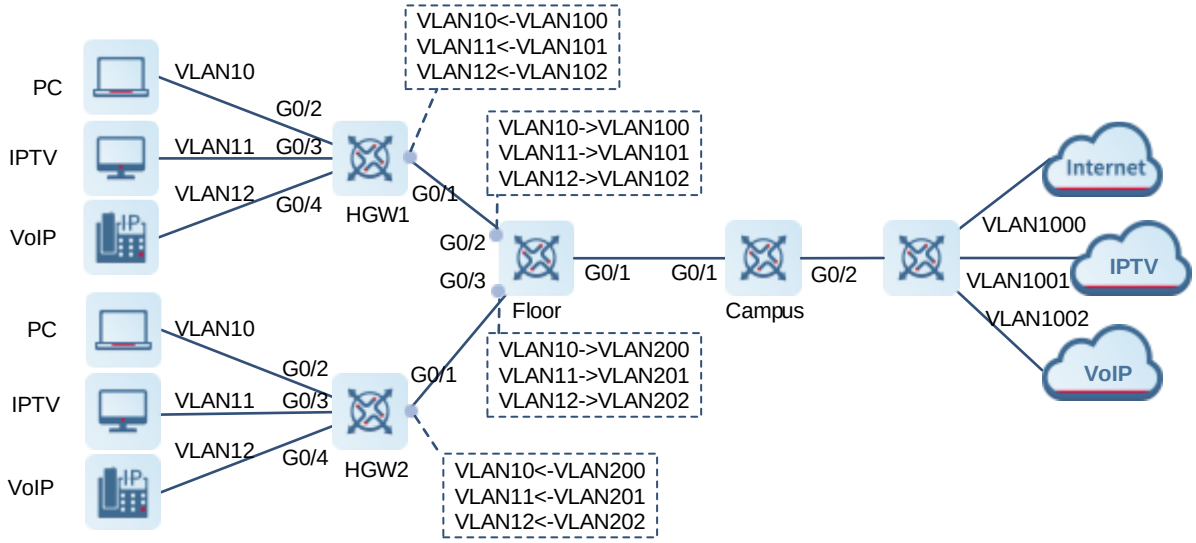
As shown in Figure 1-11, in a campus network environment, different services on the HGW are differentiated using different VLANs. VLAN 10 is used for PC services, VLAN 11 for IPTV services, and VLAN 12 for VoIP services.

For the sake of easy deployment, the same VLAN is used for the same service of HGW 1 and HGW 2, and the packets of the same service from different homes are isolated using the VLAN mapping function on the floor devices, thus avoiding confusion of the packets from different homes.

Packets of the same service from different homes are sent from campus devices through the same VLAN to save VLAN resources.

2. Topology

Figure 1-11 Configuring VLAN-Mapping to Implement Aggregation of Different Services



3. Notes

- HGW 1

  Create a VLAN after mapping, configure GigabitEthernet 0/1 as an uplink port, and configure the VLAN mapping policy for the input direction on GigabitEthernet 0/1 for the downlink data: Map VLAN 100 as VLAN 10 for forwarding to Gigabit Ethernet 0/2; map VLAN 101 as VLAN 11 for forwarding to Gigabit Ethernet 0/3; map VLAN 102 as VLAN 12 for forwarding to Gigabit Ethernet 0/4. If VLAN 200, VLAN 201, and VLAN 202 are not created, their data will be dropped even if the data is forwarded to Gigabit Ethernet 0/1.

  Configure Gigabit Ethernet 0/2, Gigabit Ethernet 0/3, and Gigabit Ethernet 0/4 as an access port, and add them to the VLAN where the corresponding service is.

- HGW 2

  Create a VLAN after mapping, configure GigabitEthernet 0/1 as an uplink port, and configure the VLAN mapping policy for the input direction on GigabitEthernet 0/1 for the downlink data: Map VLAN 200 as VLAN 10 for forwarding to Gigabit Ethernet 0/2; map VLAN 201 as VLAN 11 for forwarding to Gigabit Ethernet 0/3; map VLAN 202 as VLAN 12 for forwarding to Gigabit Ethernet 0/4. If VLAN 100, VLAN 101, and VLAN 102 are not created, their data will be dropped even if the data is forwarded to Gigabit Ethernet 0/1.

  Configure Gigabit Ethernet 0/2, Gigabit Ethernet 0/3, and Gigabit Ethernet 0/4 as an access port, and add them to the VLAN where the corresponding service is.

- Floor device

  Create a VLAN after mapping, and configure GigabitEthernet 0/1 of the floor device as an uplink port.

  Configure the downlink interface GigabitEthernet 0/2 as an uplink port, and configure the VLAN mapping policy for the input direction for the uplink data on HGW 1: Map VLAN 10 as VLAN 100; map VLAN 11 as VLAN 101; map VLAN 12 as VLAN 102. To avoid waste of the bandwidth, configure GigabitEthernet 0/2 to allow only the data of VLANs 100–102 to pass through.

  Configure the downlink interface GigabitEthernet 0/3 as an uplink port, and configure the VLAN mapping

policy for the input direction for the uplink data on HGW 2: Map VLAN 10 as VLAN 200; map VLAN 11 as VLAN 201; map VLAN 12 as VLAN 202. To avoid waste of the bandwidth, configure GigabitEthernet 0/3 to allow only the data of VLANs 200 to 202 to pass through.

- Campus device

  On Gigabit Ethernet 0/1, configure the C-tag-based QinQ encapsulation policy to encapsulate the packets of the same service with the same outer tag for transmission an access port: the data frames of VLAN 100 and VLAN 200 are encapsulated as frames of VLAN 1000 and forwarded to the Internet for communication; the data frames of VLAN 101 and VLAN 201 are encapsulated as frames of VLAN 1001 and forwarded to the IPTV network; the data frames of VLAN 102 and VLAN 202 are encapsulated as frames of VLAN 1002 and forwarded to the VoIP network.

  Configure GigabitEthernet 0/2 as an uplink port.

4. Procedure

(1) Configure HGW 1.

Create a VLAN after mapping, configure the uplink port, and configure the VLAN mapping policy for input direction for the downlink data.

```
HGW1> enable
HGW1# configure terminal
HGW1(config)# vlan range 10-12
HGW1(config-vlan-range)# exit
HGW1(config)# interface gigabitethernet 0/1
HGW1(config-if-GigabitEthernet 0/1)# switchport
HGW1(config-if-GigabitEthernet 0/1)# switchport mode uplink
HGW1(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 1
HGW1(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
HGW1(config-if-GigabitEthernet 0/1)# vlan-mapping-in vlan 100 remark 10
HGW1(config-if-GigabitEthernet 0/1)# vlan-mapping-in vlan 101 remark 11
HGW1(config-if-GigabitEthernet 0/1)# vlan-mapping-in vlan 102 remark 12
HGW1(config-if-GigabitEthernet 0/1)# exit
```

Configure the downlink interface as an access port, and add it to the VLAN where the corresponding service is.

```
HGW1(config)# interface range gigabitethernet 0/2-4
HGW1(config-if-range)# switchport
HGW1(config-if-range)# switchport mode access
HGW1(config-if-range)# exit
HGW1(config)# interface gigabitethernet 0/2
HGW1(config-if-GigabitEthernet 0/2)# switchport access vlan 10
HGW1(config-if-GigabitEthernet 0/2)# exit
HGW1(config)# interface gigabitethernet 0/3
HGW1(config-if-GigabitEthernet 0/3)# switchport access vlan 11
HGW1(config-if-GigabitEthernet 0/3)# exit
HGW1(config)# interface gigabitethernet 0/4
HGW1(config-if-GigabitEthernet 0/4)# switchport access vlan 12
HGW1(config-if-GigabitEthernet 0/4)# end
```

```
HGW1# write
```

(2) Configure HGW 2.

Create a VLAN after mapping, configure the uplink port, and configure the VLAN mapping policy for input direction for the downlink data.

```
HGW2> enable
HGW2# configure terminal
HGW2(config)# vlan range 10-12
HGW2(config-vlan-range)# exit
HGW2(config)# interface gigabitethernet 0/1
HGW2(config-if-GigabitEthernet 0/1)# switchport
HGW2(config-if-GigabitEthernet 0/1)# switchport mode uplink
HGW2(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 1
HGW2(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
HGW2(config-if-GigabitEthernet 0/1)# vlan-mapping-in vlan 200 remark 10
HGW2(config-if-GigabitEthernet 0/1)# vlan-mapping-in vlan 201 remark 11
HGW2(config-if-GigabitEthernet 0/1)# vlan-mapping-in vlan 202 remark 12
```

Configure the downlink interface as an access port, and add it to the VLAN where the corresponding service is.

```
HGW2(config)# interface range gigabitethernet 0/2-4
HGW2(config-if-range)# switchport
HGW2(config-if-range)# switchport mode access
HGW2(config-if-range)# exit
HGW2(config)# interface gigabitethernet 0/2
HGW2(config-if-GigabitEthernet 0/2)# switchport access vlan 10
HGW2(config-if-GigabitEthernet 0/2)# exit
HGW2(config)# interface gigabitethernet 0/3
HGW2(config-if-GigabitEthernet 0/3)# switchport access vlan 11
HGW2(config-if-GigabitEthernet 0/3)# exit
HGW2(config)# interface gigabitethernet 0/4
HGW2(config-if-GigabitEthernet 0/4)# switchport access vlan 12
HGW2(config-if-GigabitEthernet 0/4)# end
HGW2# write
```

(3) Configure the floor device.

Create a VLAN after mapping, and for the uplink data of HGW 1, create the VLAN mapping policy for input direction on the downlink interface.

```
Floor> enable
Floor# configure terminal
Floor(config)# vlan range 100-102
Floor(config-vlan-range)# exit
Floor(config)# interface gigabitethernet 0/2
Floor(config-if-GigabitEthernet 0/2)# switchport
Floor(config-if-GigabitEthernet 0/2)# switchport mode uplink
Floor(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
Floor(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan only 100-102
```

```
Floor(config-if-GigabitEthernet 0/2)# vlan-mapping-in vlan 10 remark 100
Floor(config-if-GigabitEthernet 0/2)# vlan-mapping-in vlan 11 remark 101
Floor(config-if-GigabitEthernet 0/2)# vlan-mapping-in vlan 12 remark 102
Floor(config-if-GigabitEthernet 0/2)# exit
```

Create a VLAN after mapping, and for the uplink data of HGW 2, create the VLAN mapping policy for input direction on the downlink interface.

```
Floor(config)# vlan range 200-202
Floor(config-vlan-range)# exit
Floor(config)# interface gigabitethernet 0/3
Floor(config-if-GigabitEthernet 0/3)# switchport
Floor(config-if-GigabitEthernet 0/3)# switchport mode uplink
Floor(config-if-GigabitEthernet 0/3)# switchport trunk native vlan 1
Floor(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan only 200-202
Floor(config-if-GigabitEthernet 0/3)# vlan-mapping-in vlan 10 remark 200
Floor(config-if-GigabitEthernet 0/3)# vlan-mapping-in vlan 11 remark 201
Floor(config-if-GigabitEthernet 0/3)# vlan-mapping-in vlan 12 remark 202
Floor(config-if-GigabitEthernet 0/3)# exit
```

Configure the uplink port.

```
Floor(config)# interface gigabitethernet 0/1
Floor(config-if-GigabitEthernet 0/1)# switchport
Floor(config-if-GigabitEthernet 0/1)# switchport mode uplink
Floor(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 1
Floor(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
Floor(config-if-GigabitEthernet 0/1)# end
Floor# write
```

(4) Configure the campus device.

Configure the C-Tag-based QinQ encapsulation rule.

```
Campus> enable
Campus# configure terminal
Campus(config)# vlan range 1000-1002
Campus(config-vlan-range)# exit
Campus(config)# interface gigabitethernet 0/1
Campus(config-if-GigabitEthernet 0/1)# switchport
Campus(config-if-GigabitEthernet 0/1)# switchport mode dot1q-tunnel
Campus(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel native vlan 1
Campus(config-if-GigabitEthernet 0/1)# switchport dot1q-tunnel allowed vlan add
untagged 1,1000-1002
Campus(config-if-GigabitEthernet 0/1)# dot1q outer-vid 1000 register inner-vid
100,200
Campus(config-if-GigabitEthernet 0/1)# dot1q outer-vid 1001 register inner-vid
101,201
Campus(config-if-GigabitEthernet 0/1)# dot1q outer-vid 1002 register inner-vid
102,202
```

Configure the uplink port.

```
Campus(config)# interface gigabitethernet 0/2
Campus(config-if-GigabitEthernet 0/2)# switchport
Campus(config-if-GigabitEthernet 0/2)# switchport mode uplink
Campus(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
Campus(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all

Campus(config-if-GigabitEthernet 0/2)# end
Campus# write
```

5. Verification

(1) Verify the configuration of HGW 1.

Display the VLAN configuration of HGW 1.

```
HGW1# show vlan
VLAN      Name                           Status    Ports
---------- --------------------------------- ---------
-----------------------------------
       1 VLAN0001                       STATIC    Gi0/1, Gi0/5, Gi0/6, Gi0/7
                                                 Gi0/8
      10 VLAN0010                       STATIC    Gi0/1, Gi0/2
      11 VLAN0011                       STATIC    Gi0/1, Gi0/3
      12 VLAN0012                       STATIC    Gi0/1, Gi0/4
```

Display the interface configuration of HGW 1.

```
HGW1# show interface switchport
Interface           Switchport Mode     Access Native Protected VLAN lists
--------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled    UPLINK         1      Disabled  ALL
GigabitEthernet 0/2   enabled    ACCESS    10          Disabled  ALL
GigabitEthernet 0/3   enabled    ACCESS    11          Disabled  ALL
GigabitEthernet 0/4   enabled    ACCESS    12          Disabled  ALL
```

Display the VLAN mapping rule of HGW 1.

```
HGW1# show interfaces vlan-mapping
Ports       type   Status     Destination-Vlan   Source-Vlan-list
-----------  -----  ---------  -----------------   -----------------
Gi0/1       in     active     10               100
Gi0/1       in     active     11               101
Gi0/1       in     active     12               102
```

(2) Verify the configuration of HGW 2.

Verify that the VLAN configuration of HGW 2 is the same as that of HGW 1.

```
HGW2# show vlan
VLAN      Name                           Status    Ports
---------- --------------------------------- ---------
-----------------------------------
       1 VLAN0001                       STATIC    Gi0/1, Gi0/5, Gi0/6, Gi0/7
```

```
                                                Gi0/8
      10 VLAN0010                       STATIC    Gi0/1, Gi0/2
      11 VLAN0011                       STATIC    Gi0/1, Gi0/3
      12 VLAN0012                       STATIC    Gi0/1, Gi0/4
```

Verify that the interface configuration of HGW 2 is the same as that of HGW 1.

```
HGW2# show interface switchport
Interface           Switchport Mode     Access Native Protected VLAN lists
--------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled    UPLINK         1      Disabled  ALL
GigabitEthernet 0/2   enabled    ACCESS    10           Disabled  ALL
GigabitEthernet 0/3   enabled    ACCESS    11           Disabled  ALL
GigabitEthernet 0/4   enabled    ACCESS    12           Disabled  ALL
```

Display the VLAN mapping rule of HGW 2. The VLAN mapping rule is different from that of HGW 1.

```
HGW2# show interfaces vlan-mapping
Ports       type   Status    Destination-Vlan   Source-Vlan-list
-----------  -----  ---------  ----------------   ----------------
Gi0/1       in     active    10              200
Gi0/1       in     active    11              201
Gi0/1       in     active    12              202
```

(3) Verify the configuration of the floor device.

Display the VLAN configuration of the floor device.

```
Floor# show vlan
VLAN      Name                            Status    Ports
---------- -------------------------------- ---------
-----------------------------------
       1 VLAN0001                        STATIC    Gi0/1, Gi0/4, Gi0/5, Gi0/6
                                                   Gi0/7, Gi0/8
   100-102 VLAN0100-VLAN0102               STATIC    Gi0/1, Gi0/2
   200-202 VLAN0100-VLAN0102               STATIC    Gi0/1, Gi0/3
```

Display the interface configuration of the floor device.

```
Floor# show interface switchport
Interface           Switchport Mode     Access Native Protected VLAN lists
--------------------- ---------- --------- ------ ------ ---------
----------------------
GigabitEthernet 0/1   enabled    UPLINK         1      Disabled  ALL
GigabitEthernet 0/2   enabled    UPLINK         1      Disabled  100-102
GigabitEthernet 0/3   enabled    UPLINK         1      Disabled  200-202
```

Display the VLAN mapping rule of the floor device.

```
Floor# show interfaces vlan-mapping
Ports       type   Status    Destination-Vlan   Source-Vlan-list
-----------  -----  ---------  ----------------   ----------------
Gi0/2       in     active    100             10
```

```
Gi0/2       in    active    101             11
Gi0/2       in    active    102             12
Gi0/3       in    active    200             10
Gi0/3       in    active    201             11
Gi0/3       in    active    202             12
```

(4) Verify the configuration of the campus device.

Display the interface configuration.

```
Campus# show interfaces switchport
Interface                    Switchport Mode     Access Native Protected VLAN
lists
-------------------------------- ---------- --------- ------ ------ ---------
----------------
GigabitEthernet 0/1            enabled    TUNNEL        1     Disabled
1,1000-1002
GigabitEthernet 0/2            enabled    UPLINK        1     Disabled  ALL
```

Display the dot1q-tunnel configuration. The outer tag VLAN has been added to the allowed VLAN list of the interface.

```
Campus# show interfaces dot1q-tunnel
========Interface Gi0/1========
Native vlan: 1
Allowed vlan list:1,1000-1002
Tagged vlan list:
```

Display the mapping policy relationship for adding S-tags based on C-tags.

```
Campus# show registration-table
Ports     Type           Outer-VID    Inner-VID-list
------    ----------      ----------   --------------
Gi0/1     Add-outer      1000          100,200
Gi0/1     Add-outer      1001          101,201
Gi0/1     Add-outer      1002          102,202
```

6. Configuration Files

- Configuration file of HGW 1

```
vlan range 1,10-12
!
interface GigabitEthernet 0/1
switchport
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094vlan-mapping-in vlan 100 remark 10
 vlan-mapping-in vlan 101 remark 11
 vlan-mapping-in vlan 102 remark 12
!
interface GigabitEthernet 0/2
switchport
```

```
 switchport mode accessswitchport access vlan 10
!
interface GigabitEthernet 0/3
switchport
 switchport mode access
switchport access vlan 11
!
interface GigabitEthernet 0/4
switchport
 switchport mode access
switchport access vlan 12
```

- Configuration file of HGW 2

```
vlan range 1,10-12
!
interface GigabitEthernet 0/1
switchport
switchport mode uplink
 switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
 vlan-mapping-in vlan 200 remark 10
 vlan-mapping-in vlan 201 remark 11
 vlan-mapping-in vlan 202 remark 12
!
interface GigabitEthernet 0/2
switchport
 switchport mode access
switchport access vlan 10
!
interface GigabitEthernet 0/3
 switchport
 switchport mode access
switchport access vlan 11
!
interface GigabitEthernet 0/4
 switchport
 switchport mode access
switchport access vlan 12
```

- Configuration file of the floor device

```
vlan range 1,100-102,200-202
!
interface GigabitEthernet 0/1
switchport
 switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

```
!
interface GigabitEthernet 0/2
 switchport
 switchport mode uplink
 switchport trunk native vlan 1
switchport trunk allowed vlan only 100-102
vlan-mapping-in vlan 10 remark 100
 vlan-mapping-in vlan 11 remark 101
 vlan-mapping-in vlan 12 remark 102
!
interface GigabitEthernet 0/3
 switchport
 switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 200-202
vlan-mapping-in vlan 10 remark 200
 vlan-mapping-in vlan 11 remark 201
 vlan-mapping-in vlan 12 remark 202
```

- Configuration file of the campus device

```
vlan range 1,1000-1002
!
interface GigabitEthernet 0/1
 switchport
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 1,1000-1002
 switchport dot1q-tunnel native vlan 1dot1q outer-vid 1000 register inner-vid
100,200
 dot1q outer-vid 1001 register inner-vid 101,201
dot1q outer-vid 1002 register inner-vid 102,202
!
interface GigabitEthernet 0/2
 switchport
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

1.14.5 Configuring Layer-2 Protocol Tunneling Based on QinQ

1. Requirements

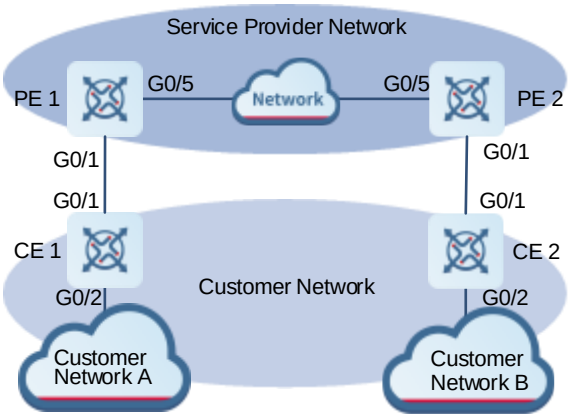
As shown in Figure 1-12, the upper part of the typical topology of QinQ network is the SP network, and the lower part is the client network. The SP network consists of PE 1 and PE 2. Customer Network A and Customer Network B are a user's two sites in different regions. CE 1 and CE 2 are access devices 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 1-12 Configuring QinQ to Implement 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 "1.14.1 Configuring Basic QinQ to Implement Layer-2 VPN") to configure the native VLAN of dot1q-tunnel 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 of PE 1 and PE 2.
- Configure the uplink port of PE 1 and PE 2.

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 dot1q-tunnel, and belongs to the allowed untagged VLAN list of the dot1q-tunnel.

```
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 dot1q-tunnel.

```
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

Verify that the STP tunneling function is enabled globally and on the interface at the same time. c

```
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. The verification methods on PE1 and PE2 are the same. PE1 is taken as an example.

Verify PE 1.

```
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
 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
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

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 STP 5
1.1 Introduction 5
1.1.1 Overview 5
1.1.2 Background and Functions 6
1.1.3 STP 7
1.1.4 RSTP 17
1.1.5 MSTP 23
1.1.6 MVST 32
1.1.7 Rapid-MVST 37
1.1.8 Protocols and Standards 38
1.2 Restrictions and Guidelines 39
1.3 Configuration Task Summary 39
1.3.1 Configuring STP 39
1.3.2 Configuring RSTP 39
1.3.3 Configuring MSTP 39
1.3.4 Configuring Advanced Functions for Spanning Trees 40
1.3.5 Configuring BPDU Transparent Transmission 40
1.3.6 Configuring MVST 41
1.3.7 Configuring Rapid-MVST 41
1.4 Configuring the Spanning Tree Mode 41
1.4.1 Overview 41
1.4.2 Restrictions and Guidelines 41

1.4.3 Procedure....41
1.5 Configuring an MST Region....42
1.5.1 Overview....42
1.5.2 Restrictions and Guidelines....42
1.5.3 Prerequisites....42
1.5.4 Procedure....42
1.6 Configuring the Bridge Priority and Port Priority....43
1.6.1 Overview....43
1.6.2 Restrictions and Guidelines....43
1.6.3 Prerequisites....44
1.6.4 Procedure....44
1.7 Configuring the Port Path Cost....44
1.7.1 Overview....44
1.7.2 Configuration Tasks....45
1.7.3 Configuring the Path Cost Calculation Method....45
1.7.4 Configuring the Path Cost Value....46
1.8 Configuring Spanning Tree Time Parameters....47
1.8.1 Overview....47
1.8.2 Restrictions and Guidelines....47
1.8.3 Procedure....48
1.9 Configuring the Maximum Hop Count for BPDUs....48
1.9.1 Overview....48
1.9.2 Restrictions and Guidelines....49
1.9.3 Procedure....49

1.10 Configuring Fast Convergence of Spanning Trees 49
1.10.1 Overview 49
1.10.2 Restrictions and Guidelines 49
1.10.3 Prerequisites 50
1.10.4 Procedure 50
1.11 Enabling Protocol Migration 50
1.11.1 Overview 50
1.11.2 Procedure 51
1.12 Configuring Spanning Tree Compatibility for Interfaces 51
1.12.1 Overview 51
1.12.2 Prerequisites 51
1.12.3 Procedure 51
1.13 Enabling the STP Function 52
1.13.1 Overview 52
1.13.2 Restrictions and Guidelines 52
1.13.3 Procedure 52
1.14 Configuring Port Protection 52
1.14.1 Overview 52
1.14.2 Restrictions and Guidelines 53
1.14.3 Configuration Tasks 53
1.14.4 Configuring Root Guard 53
1.14.5 Configuring Loop Guard 54
1.15 Configuring BPDU Source MAC Address Check 55
1.15.1 Overview 55

1.15.2 Restrictions and Guidelines 56
1.15.3 Prerequisites 56
1.15.4 Procedure 56
1.16 Configuring an Edge Port 56
1.16.1 Overview 56
1.16.2 Restrictions and Guidelines 57
1.16.3 Configuration Tasks 57
1.16.4 Configuring Autoedge 57
1.16.5 Configuring the Port Fast Attribute 58
1.17 Configuring BPDU Guard or BPDU Filter 59
1.17.1 Overview 59
1.17.2 Restrictions and Guidelines 59
1.17.3 Configuration Tasks 60
1.17.4 Configuring BPDU Guard 60
1.17.5 Configuring BPDU Filter 61
1.18 Configuring TC Attack Defense Functions 62
1.18.1 Overview 62
1.18.2 Restrictions and Guidelines 63
1.18.3 Configuration Tasks 63
1.18.4 Configuring TC Protection 63
1.18.5 Configuring TC Guard 64
1.18.6 Configuring TC Filter 65
1.19 Configuring BPDU Tunnel 66
1.19.1 Overview 66

1.19.2 Restrictions and Guidelines 66
1.19.3 Prerequisites 66
1.19.4 Procedure 67
1.20 Configuring BPDU Transparent Transmission 67
1.20.1 Overview 67
1.20.2 Restrictions and Guidelines 67
1.20.3 Procedure 68
1.21 Configuring STP in the Specified VLAN 68
1.21.1 Overview 68
1.21.2 Restrictions and Guidelines 68
1.21.3 Procedure 68
1.22 Monitoring 69
1.23 Configuration Examples 70
1.23.1 Configuring MSTP 70
1.23.2 Configuring MSTP+VRRP 86
1.23.3 Configuring Spanning Tree Compatibility for MSTP Interfaces 102
1.23.4 Configuring BPDU Tunnel 108
1.23.5 Configuring BPDU Transparent Transmission 116
1.23.6 Configuring MVST 121

1 Configuring STP

1.1 Introduction

1.1.1 Overview

The Spanning Tree Protocol (STP) is a Layer 2 management protocol used to eliminate Layer 2 loops by blocking redundant links in the network. It enables a backup link in the case of a link failure.

As the network evolves, multiple STP versions become available. This device supports STP, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Multiple VLAN Spanning Tree (MVST), and Rapid Multiple VLAN Spanning Tree (Rapid-MVST).

1.1.2 Background and Functions

1. 802.1D STP

To prevent single point of failures (SPOFs), Layer 2 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 block certain interfaces through calculations to generate an optimal loop-free topology of a LAN. If a line fault is detected, STP restores the blocked interfaces, enables the backup link, and updates the topology automatically.

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 Layer 2, and Layer 2 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 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 Layer 2 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 generate multiple spanning trees by VLAN instance to implement traffic balancing.

4. MVST

MVST is a spanning tree protocol developed based on the Electrical and Electronics Engineers (IEEE) 802.1D standard and allows you to enable spanning tree separately in multiple VLANs. Different from STP, RSTP, or MSTP, you need to enable spanning tree loop-prevention in the specified VLAN on demand when you use MVST. Spanning tree calculation takes effect only in the VLANs with spanning tree enabled.

5. Rapid-MVST

As an improvement to MVST, Rapid-MVST introduces the quick handshake proposal/agreement mechanism defined in IEEE 802.1w to achieve the effects of fast convergence.

1.1.3 STP

1. Overview

STP, defined by the Institute of 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.

Layer 2 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, a Layer 2 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 a Layer 2 loop, it will be flooded continuously by Layer 2 devices and a broadcast storm will be incurred, which will heavily consume device resources and network bandwidth.
- In a loop topology, a Layer 2 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 Layer 2 Ethernet, only one valid channel is required to forward data between two LANs. Ideally, when a Layer 2 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 1.1.3 3. 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

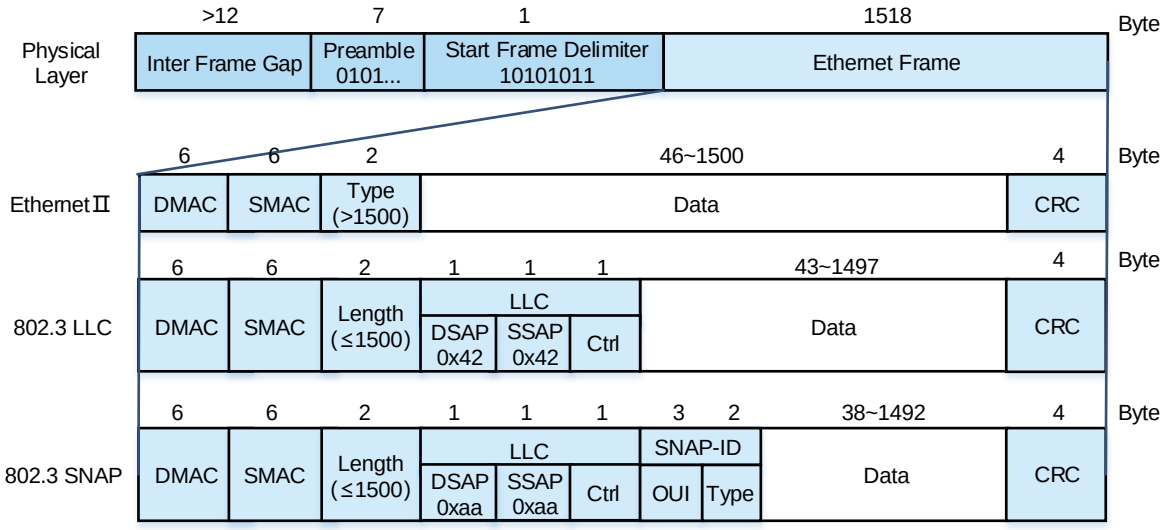
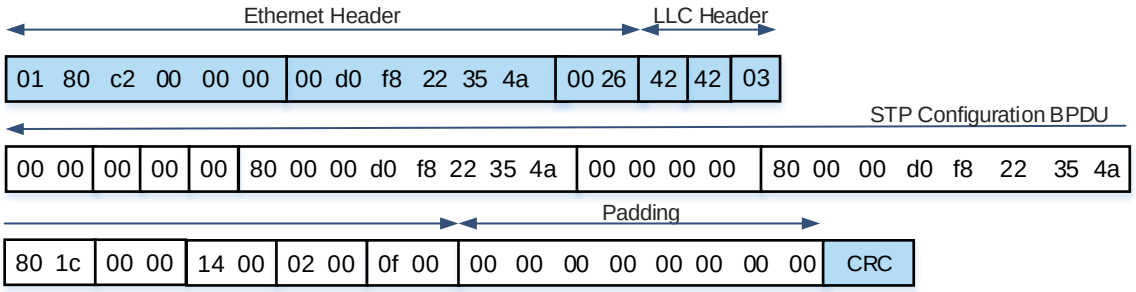


Figure 1-2 is an actual STP configuration BPDU taken as an example.

Figure 1-2 STP Configuration BPDU



The header of an IEEE 802.3 Ethernet frame contains 14 bytes in three fields in the header, as 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.
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 in three fields, as 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 in 12 fields, as described in Table 1-3. The last part is an 8-byte filling field and a 4-byte CRC field. 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.

Field	Bytes	Description
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.
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 ID**, **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
-	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

- 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.
- Blocking port: A port on a non-root bridge that is in the blocking state.
- Disable port: A port in the Down state.

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

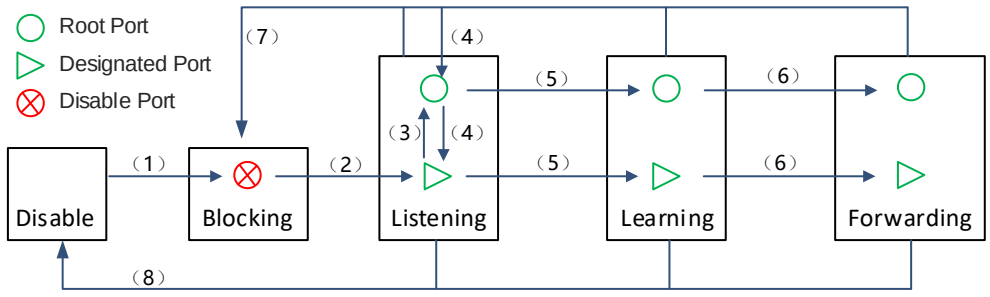
Note: In this table, R = root port, D = designated port, Blk=Blocking port, A = alternate port, B = backup port.

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 user. 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 (which is the 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

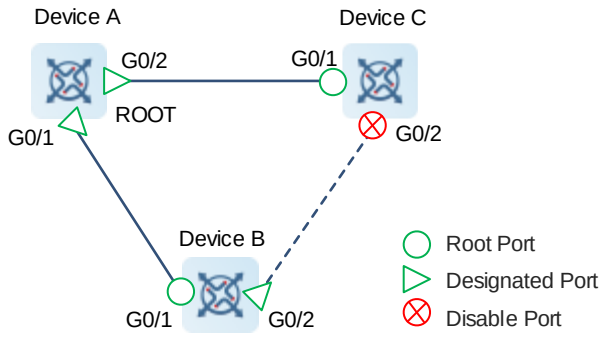
state to learn MAC addresses. After waiting for another period of **Forward Delay**, the designated ports transition from learning state to forwarding state and start receiving and sending packets.

(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. The priority vector in the configuration BPDU packet sent by the interface is <RID, Cost, BID, PID>, and that saved by the interface 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**, GigabitEthernet 0/2 transitions to learning state to learn MAC addresses. After waiting for another period of **Forward Delay**, 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

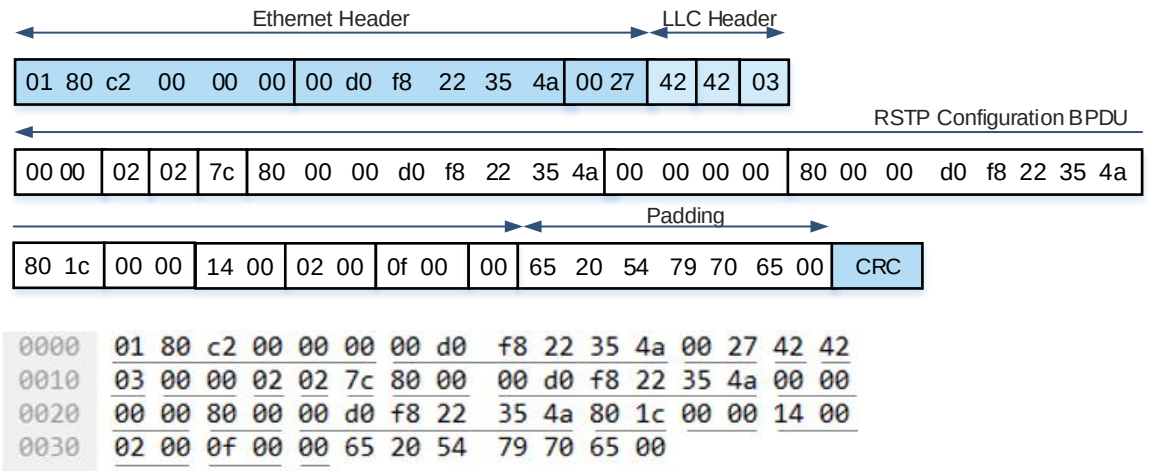
RSTP, defined by IEEE 802.1W, evolves from STP and is compatible with IEEE 802.1D STP downward. RSTP has all functions of the conventional STP protocol and is capable of preventing loops and providing redundant links. Compared with STP, RSTP shortens the time required for network topology convergence. 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



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 fields of a RST BPDU packet are described in Table 1-8. The 39 bytes, plus the last 7 padding bytes and the 4 CRC bytes, together form a 64 byte Ethernet frame.

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.
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.

Field	Bytes	Description
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:

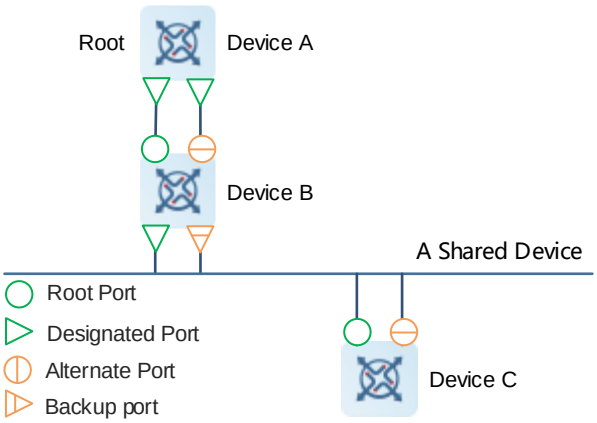
- Root port: A port with the shortest path to the root bridge.
- Alternate port: A backup port of a root port. Once the root port fails, the alternate port becomes the root port immediately.
- Designated port: A port that connects a root bridge or upstream bridge to a downstream device.
- Backup port: 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

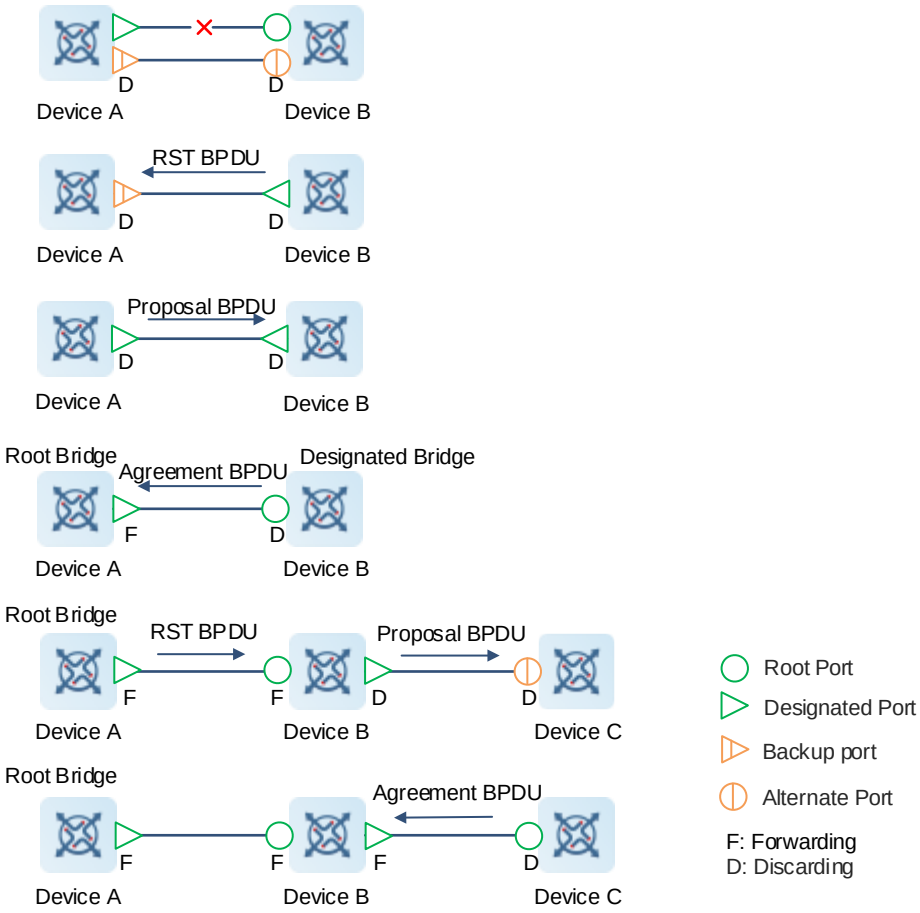
In RSTP, a device processes BPDUs in a different way.

- 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.

(3) 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.

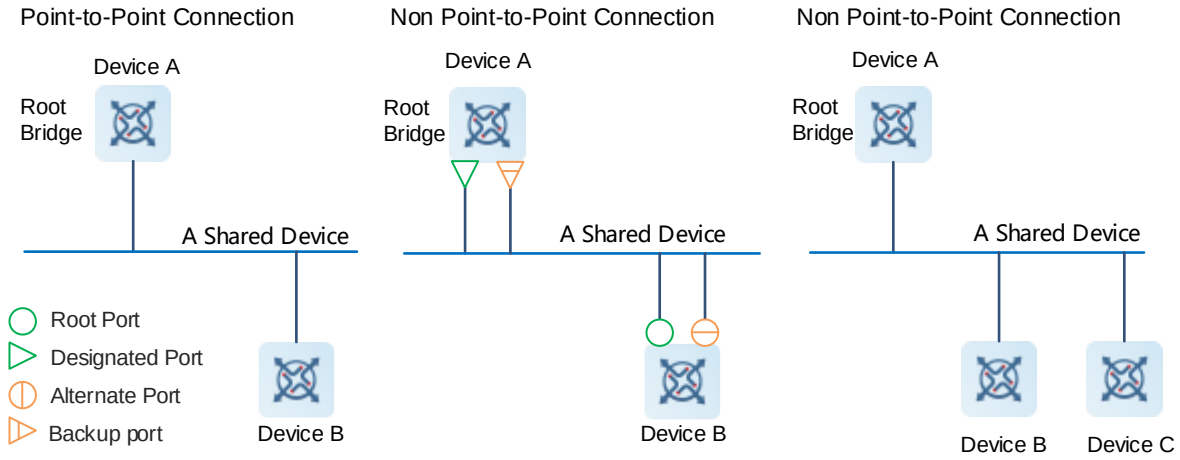
(4) Extension proposal: The designated port of Device B sends a Proposal BPDU with both **Proposal** and **Agreement** bits set to **1** to the downstream device, to request the downstream device to recognize Device B as the upstream device and extend the spanning tree. Theoretically, RSTP can recover 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 creates 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 Multiple VLAN Spanning Tree (MVST) (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.

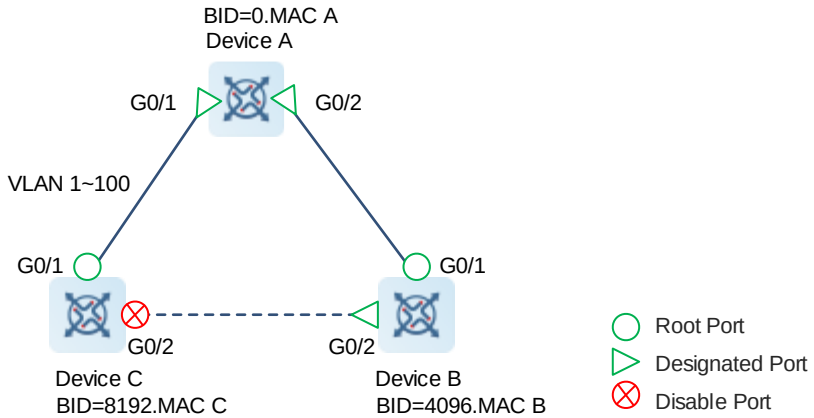
2. Origin of MSTP

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.

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.

Figure 1-9 Traffic Sharing Failure in STP

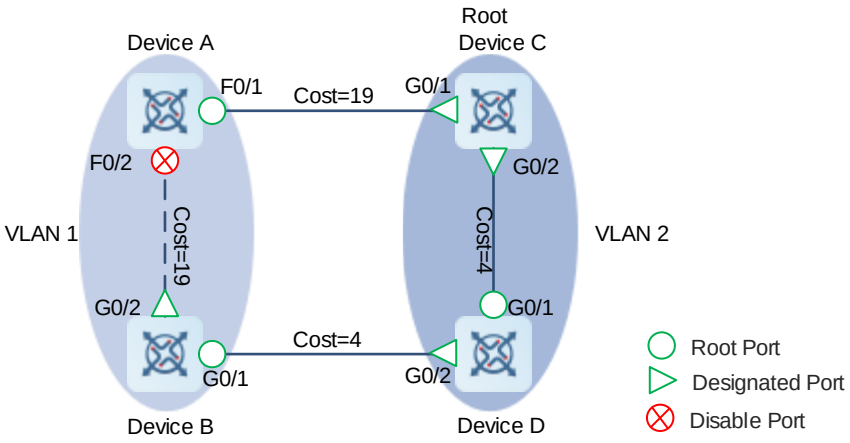


- In special cases, STP and RSTP may block links in the same VLAN, causing interfaces within the same

VLAN to be unable to communicate with each other.

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.

Figure 1-10 Communication Failure in the Same VLAN Caused by STP



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.

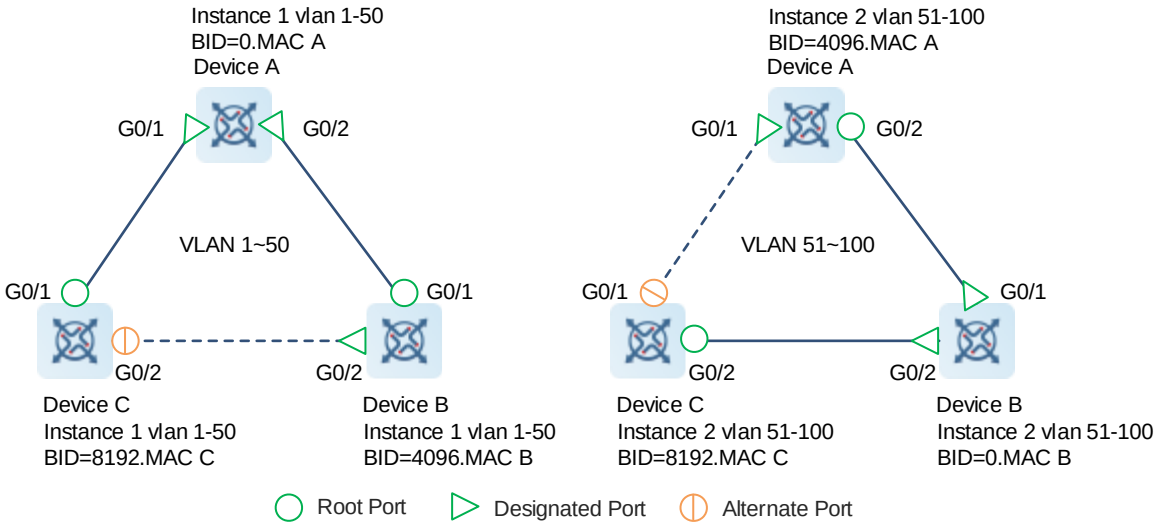
⚠ Caution

"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.

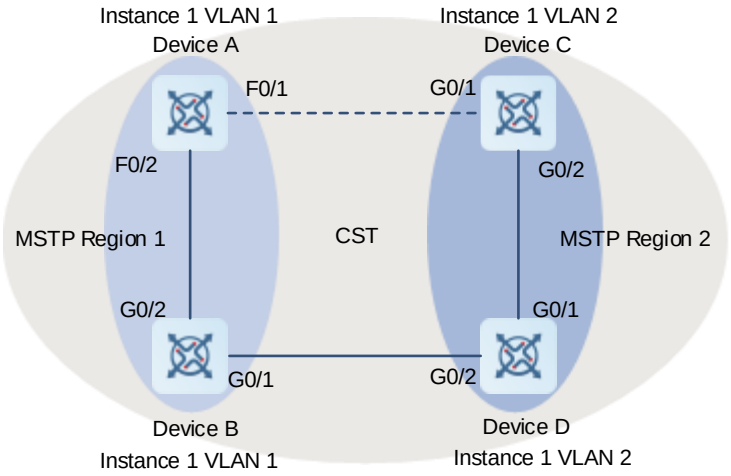
Users can, as needed, configure different instances for different VLAN groups, Configuring the Bridge Priority and Port Priority by instance, Configuring the Port Path Cost, and plan VLAN groups to forward traffic through different paths.

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

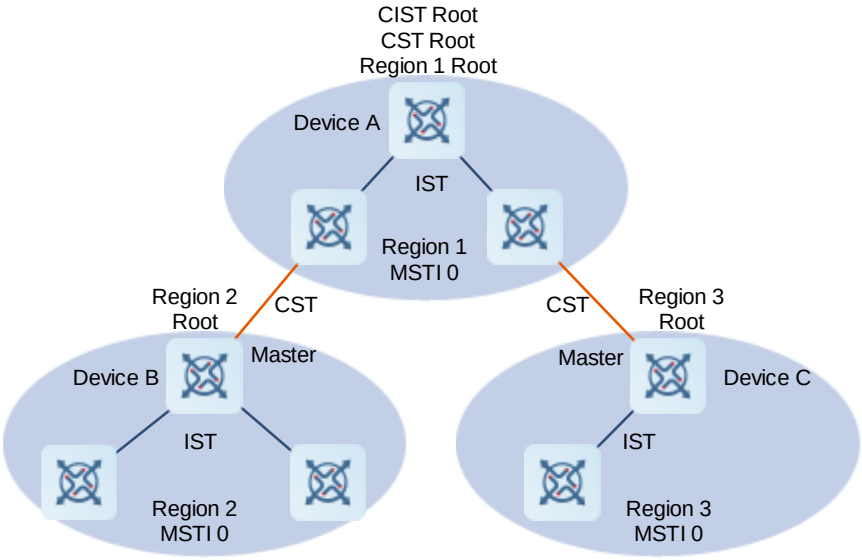
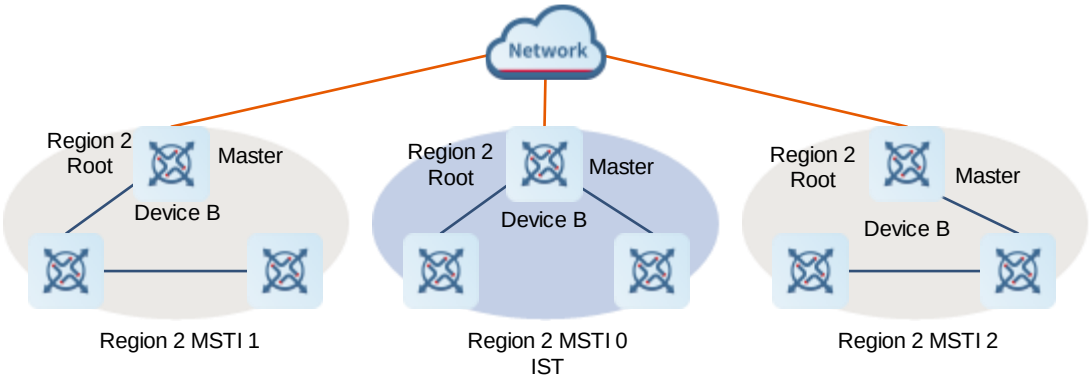


Figure 1-14 Three Spanning Trees Generated for the Three Instances in Region 2



8. Port Roles

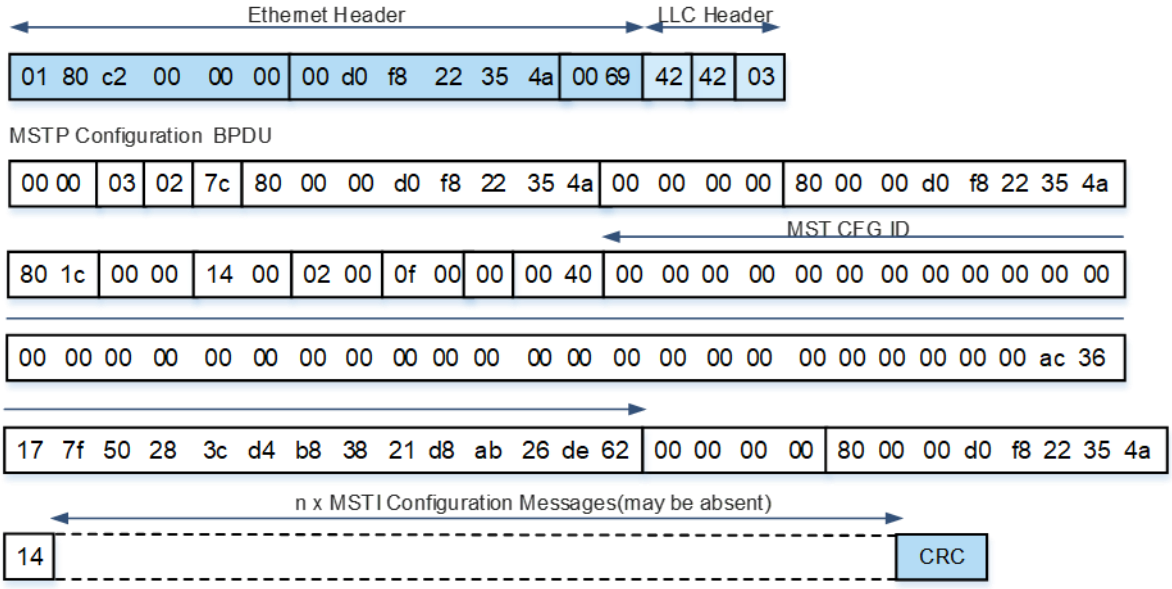
MSTP introduces a new port role to the region root: master port, which is the port with the smallest root path cost from a region to the CIST root. The master port is the "outlet" of all instances in a region, and all instances can forward data through the master port.

- 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



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.
Message Age	2	Age of a BPDU, that is, keepalive time of the packet. The value is 0x0000 in the example.

Field	Bytes	Description
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.
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 MVST

1. Overview

MVST is a spanning tree protocol developed based on the IEEE 802.1D standard and allows you to enable spanning tree separately in multiple VLANs. Featuring flexible deployment, you can enable loop-prevention in one or more VLANs based on actual needs.

The differences among STP, RSTP, MSTP and MVST are as follows:

- STP and RSTP must be enabled in the global configuration mode and spanning tree is calculated by interface. There is only one spanning tree globally and the interface in all the VLANs is in the same STP forwarding state.
- MSTP must be enabled in the global configuration mode, but VLANs can be bound to MSTP instances, with each instance calculating the spanning tree separately.
- MVST can be enabled by VLAN. If an interface is added to a VLAN, the interface participates in spanning tree calculation of this VLAN. Otherwise, the interface does not participate in the spanning tree calculation.

Developed based on IEEE 802.1D, MVST uses a processing mechanism similar to that of STP:

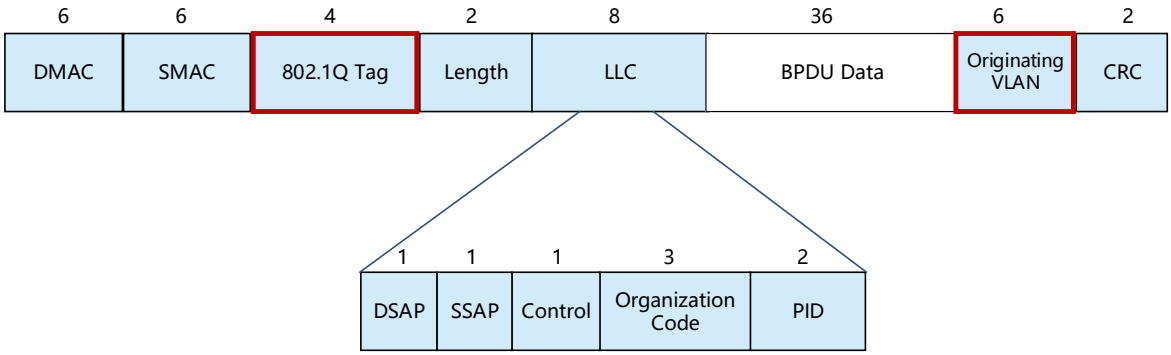
- Devices enabled with MVST exchange specific MVST Protocol Packets that are encapsulated by BPDU. Different from STP, MVST BPDUs are encapsulated in the IEEE 802.3 SNAP format. MVST elects the device roles (root bridge and non-root bridge) and port roles (root port, designated port, and blocking port) based on key information of BPDUs. Different port roles are in different port states and have different functions. They form a spanning tree topology in a VLAN.
- Protocol packets are used to monitor the line status to maintain the spanning tree topology.
- Once a fault is detected and restored, MVST automatically updates the spanning tree topology.

2. MVST Protocol Packets

The same as STP, MVST uses two types of protocol packets: configuration BPDU and TCN BPDU.

The configuration BPDU and TCN BPDU of MVST are similar to those of STP, with the following differences: MVST packets are encapsulated in the IEEE 802.3 SNAP format (as shown in Figure 1-1). 802.1Q VLAN tags are inserted to MVST packets based on the VLAN in which MVST is enabled. The **Originating VLAN** field is added to the end of STP configuration BPDU for carrying the MVST VLAN information.

Figure 1-1 Encapsulation Structure of MVST BPDUs



- Configuration BPDU

  The length of a packet is 64 bytes with no IEEE 802.1Q tag encapsulated and is 68 bytes with an IEEE 802.1Q tag encapsulated. Configure BPDU to contain information used to calculate the STP topology, including the root bridge ID, root path metric, designated bridge ID, designated port ID, and the information used to maintain the STP, such as **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

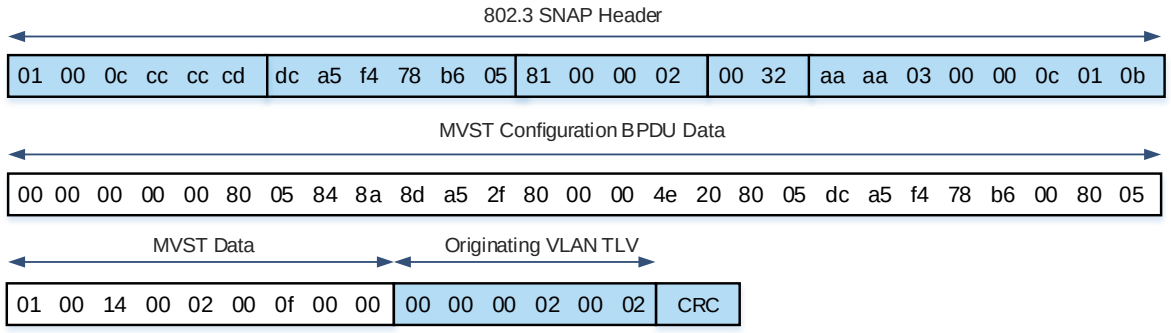
port on the device, and the designated ports generate their own BPDUs. If the configuration BPDU received by a designated port from the line has a lower priority than the BPDU generated by the designated port itself (see 1.1.3 3. Key Information of BPDUs), the designated port sends its BPDU to the downstream device.

- TCN BPDU

  A TCN BPDU contains 60 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.

Figure 1-2 shows the constitution of MVST configuration BPDUs.

Figure 1-2 MVST Configuration BPDU



The IEEE 802.3 Ethernet header with a length of 14 bytes has three fields when it is not encapsulated with an IEEE 802.1Q tag. Otherwise, the header has four fields and a length of 18 bytes. The packet in the example is encapsulated with an IEEE 802.1Q tag. Table 1-1 shows the field description.

Table 1-1 Description of Fields in the Header of an IEEE 802.3 Ethernet Frame

Field	Bytes	Description
DMAC	6	Destination MAC address. For an Ethernet frame with MVST-encapsulated BPDU, it has a fixed destination address of multicast address 0100.0ccc.cccd. Such frames are not forwarded once received by a device.
SMAC	6	Source MAC address of the device sending the BPDU. The value in the example is dca5.f478.b605.

Field	Bytes	Description
802.1Q Tag	4	Field added according to IEEE 802.1Q. Whether this field is encapsulated depends on the configuration of the interface and VLAN. For details, see *Configuring VLAN*. In the example, the complete value of this field is **0x81000002**. This field includes the following information: ● Type: 2-byte field. The value **0x8100** identifies an IEEE 802.1Q frame. In the example, the packet is encapsulated with an 802.1Q tag, so the corresponding field value is **0x8100**. ● PRI: 3-bit field, indicating the Layer 2 priority. The value range is from 0 to 7, corresponding to the CoS priority of QoS. A larger value indicates a higher priority. The value is **0** in the example. ● CFI: 1-bit field used to distinguish Ethernet frames, FDDI frames, and token ring frames. **0** indicates an Ethernet frame. The value is **0** in the example. VID: 12-bit field. 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. The value is **2** in the example.
Length	2	The value is **0x0032**, indicating that the packet length is 50 bytes (the LLC header occupies 8 bytes, the BPDU packet occupies 36 bytes, and the originating VLAN TLV occupies 6 bytes).

The LLC header consists of 8 bytes, which is SNAP encapsulated and divided into 5 fields.Table 1-2 shows the field description.

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 0xaa.
SSAP	1	Source service access point. The value is 0xaa.
Control	1	This field stores various control information and identifies the type of an LLC frame. The value is 0x03.
OUI	3	Organization unique identifier, which is **0x00000c**.
PID	1	Protocol ID. The value of this field in MVST packets is **0x010b**.

The bytes following the LLC header is a BPDU. The BPDU packet format and content of MVST is generally the same as that of STP, except that one more bit is added at the end.Table 1-3 shows the field description.

Table 1-3 Format of an MVST Configuration BPDU

Field	Bytes	Description
PID	2	Protocol identifier. The value is 0x0000.
PVID	1	Protocol version identifier. 0x00 indicates an STP packet.

Field	Bytes	Description
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.
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.
Reserved	1	Reserved. The value is **0x00**.

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 MVST 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.

The Originating VLAN TLV field is 6 bytes long and is added only after BPDU packets of MVST. Table 1-5 shows the format.

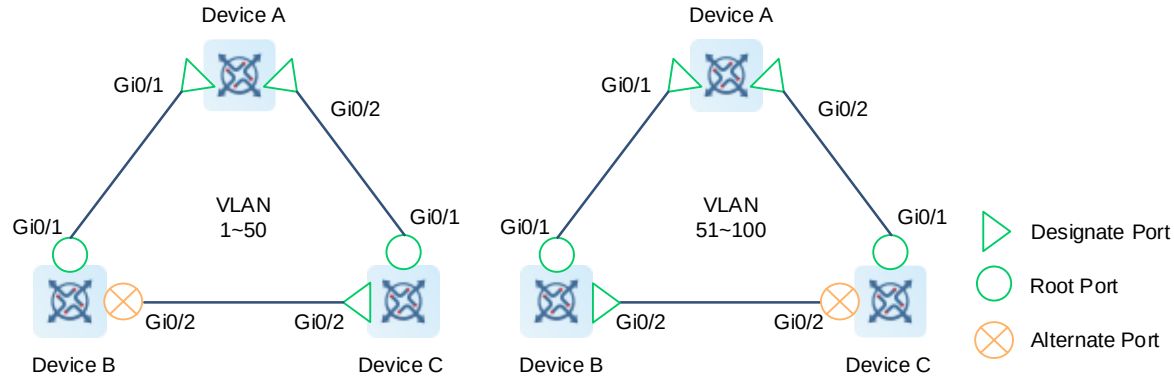
Table 1-5 Originating VLAN TLV Format

Field	Bytes	Description
Type	2	Type. The value for the originating VLAN TLV is **0x0000**.
Length	2	Total length of valid fields following this field. The value is **0x02** for the originating VLAN TLV.
Originating VLAN	2	VLAN ID of the packet sender. The value is **0x02** in the example, indicating that the VLAN ID of the packet sender is 2.

3. BPDU Processing of MVST

The calculation method of MVST is basically the same as that of STP. On the basis of STP, MVST further supports spanning tree calculation by VLAN and allows users to adjust the bridge priority of each network bridge in a specific VLAN on demand to block different interfaces in different spanning trees for different VLANs, implementing VLAN-based load balancing. In the topology as shown in**Figure 1-3**, in VLANs 1–50, you can adjust the priorities of the devices to make Device A the root bridge, Device C with the second-highest priority, and Device B with the lowest priority, thus blocking Device B. In VLANs 51–100, you can adjust the priorities of the devices to make Device A the root bridge, Device B with the second-highest priority, and Device C with the lowest priority, thus blocking Device C.

Figure 1-3 Traffic Balancing Using MVST



1.1.7 Rapid-MVST

1. Overview

Rapid-MVST is developed based on the IEEE 802.1w standard, and it is derived from and backward compatible with MVST. Rapid-MVST supports all functions of MVST and can prevent loops and provide link redundancy. Compared with MVST, Rapid-MVST takes less time to converge the network topology. If all network bridges in a LAN support Rapid-MVST and all the configurations are proper, it takes less than 1 second for Rapid-MVST to regenerate a topology tree in case of network topology changes. However, MVST requires about 50 seconds.

2. Rapid-MVST Protocol Packets

Similar to RSTP, Rapid-MVST needs only one type of protocol packet: configuration BPDU. The packet format is the same as that of MVST configuration BPDU and is called Rapid-MVST BPDU in the following parts. **Table 1-6**lists the differences between MVST configuration BPDU and Rapid-MVST configuration BPDU.

Table 1-6 Differences Between MVST Configuration BPDU and Rapid-MVST Configuration BPDU

Field	MVST Configuration BPDU	Rapid-MVST Configuration BPDU
PVID	0x00	0x02
BPDU Type	0x00	0x02

Field	MVST Configuration BPDU	Rapid-MVST Configuration BPDU
Flags	MVST configuration BPDUs use only bits 7 and 0, and other bits are not used. ● 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 0: TC. [[!100!]]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.	Rapid-MVST BPDUs use all the eight bits. ● 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.
Reserved	This field is not used in MVST configuration BPDUs and is filled with 0x00.	In Rapid-MVST, this field indicates ver 1 length. For details, see .Table 1-8

Rapid-MVST no longer notifies topology changes through MVST TCN BPDUs. Instead, the TC bit in the **Flags** field of Rapid-MVST BPDU is set to 1 to quickly instruct network-wide devices to perform topology convergence through the TC packet.

3. Fast Convergence of Rapid-MVST

Similar to RSTP, Rapid-MVST adopts a calculation method defined in the IEEE 802.1D standard. The difference is that RSTP is applied to an interface but Rapid-MVST is applied to interfaces added to a VLAN. In addition, Rapid-MVST uses the Proposal/Agreement mechanism to quickly enter the forwarding state through Proposal/Agreement handshake with the directly connected network bridge. The working principles are as the same as those of RSTP. For details on the process, see section 1.1.4 5. Fast Convergence of RSTP.

1.1.8 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 Restrictions and Guidelines

- The MSTP feature only takes effect on a Layer 2 interface. A Layer 3 interface cannot be directly configured as a dot1q tunnel port, and must be configured as a Layer 2 interface first.
- You can use the **show interface switchport** command to view the interface type. If the Switchport field corresponding to the interface is "enabled", it means that the interface is a Layer 2 interface. If the Switchport field corresponding to the interface is "disabled", it means that the interface is a Layer 3 interface.
- You can use the **switchport** command to configure the interface as a Layer 2 interface. First, use the **no switchport mode** command to restore the mode of the Layer 2 interface to the default value, and then use the **no switchport** command to configure the Layer 2 interface as a Layer 3 interface. When the Layer 2/Layer 3 mode of the interface is modified, all properties of the interface are restored to the default values of the interface type.

1.3 Configuration Task Summary

1.3.1 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

1.3.2 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

1.3.3 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

1.3.4 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

1.3.5 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

1.3.6 Configuring MVST

The MVST 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.

(4) Configuring the Path Cost Calculation Method

(5) Configuring the Path Cost Value

(6) (Optional) Configuring Spanning Tree Time Parameters

(7) Enabling the STP Function

1.3.7 Configuring Rapid-MVST

The Rapid-MVST 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.

(4) Configuring the Path Cost Calculation Method

(5) Configuring the Path Cost Value

(6) (Optional) Configuring Spanning Tree Time Parameters

(7) (Optional) Configuring Fast Convergence of Spanning Trees

(8) (Optional) Enabling Protocol Migration

(9) Enabling the STP Function

1.4 Configuring the Spanning Tree Mode

1.4.1 Overview

According to IEEE 802.1 protocol standards, STP, RSTP, and MSTP are mutually compatible, without any configuration by the user. Spanning trees generated using MVST or Rapid-MVST may not be compatible with those generated using STP, RSTP, or MSTP. Therefore, a spanning tree mode can be configured to resolve the incompatibility that occurs when the devices of some vendors do not implement the standards. Users can switch the spanning tree mode to a lower version if devices of other vendors are incompatible with this device.

1.4.2 Restrictions and Guidelines

- 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.

1.4.3 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** | **mvst** | **rapid-mvst** | **rstp** | **stp** }

The default spanning tree mode is MSTP.

1.5 Configuring an MST Region

1.5.1 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.

1.5.2 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. By default, all VLANs are in Instance 0. In MST configuration mode, you can use the **instance instance**-*id* **vlan vlan**-*range* command to move the VLAN *vlan-range* to the *instance-id*. *instance-id* indicates the spanning tree instance number. The value range is 0-64. VLAN range refers to the list of VLAN IDs. The value range is 1-4094.
- You can use the **no instance** *instance-id* or **default instance** *instance-id* command to delete an instance (not Instance 0), and move all VLANs in the instance (not Instance 0) to Instance 0. The value of *instance-id* cannot be 0, and the value range is 1-64.
- You can use the **no instance** *instance-id* **vlan** *vlan-range* command (with the parameter **vlan** *vlan-range*) to move all VLANs in the instance (not Instance 0) to Instance 0. The value of *instance-id* cannot be 0, and the value range is 1-64. If there are multiple VLANs in a specified instance, you can use the command with parameter to move some VLANs to Instance 0, and some VLANs remain in the specified instance. If all VLANs in the specified instance are moved to Instance 0, the specified instance will be automatically deleted.

1.5.3 Prerequisites

Only MSTP supports instance configuration. If the spanning tree mode is not MSTP, 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.

1.5.4 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 Create an instance, and move the VLAN from the original instance to this 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 an empty string.

(4) (Optional) Configure a revision number for the MST region.

revision *version*

The default revision number of an MST region is **0**.

1.6 Configuring the Bridge Priority and Port Priority

1.6.1 Overview

The bridge priority concerns the root bridge election as well as the topology of the entire network. Configure the bridge priority when the user 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. 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. Configure the port priority when the user needs to change ports entering forwarding state.

1.6.2 Restrictions and Guidelines

- In **mst** *instance-id*, the value range of an instance ID is from 0 to 64 and the default value is **0**. When the spanning tree works in STP/RSTP mode, the instance ID can only be 0.
- The **vlan** *vlan-list* option can be used in MVST and Rapid-MVST modes. The *vlan-list* parameter indicates a string of VLAN IDs, such as 1–10,20–30,40,50.
- The options of bridge priority indicated by **priority** include 16 values, all of 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 user 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.

> **Caution**
>
> When the device is in MVST or Rapid-MVST mode, reducing the bridge priority of the root bridge is a high-risk operation. This operation triggers a re-election for the root bridge in the spanning tree. During the election, the spanning tree status of the port experiences temporary flapping and intermittent traffic interruption occurs.

- 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.

1.6.3 Prerequisites

- Configure the interface as a Layer 2 interface.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the bridge priority.

spanning-tree [**mst** *instance-id* | **vlan** *vlan-list*] **priority** *priority*

The default bridge priority is **32768**.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(5) Configure the port priority.

spanning-tree [**mst** *instance-id* | **vlan** *vlan-list*] **port-priority** *port-priority*

The default port priority is **128**.

1.7 Configuring the Port Path Cost

1.7.1 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 user can configure the port path cost to determine the port or path, through which packets pass preferentially.

1.7.2 Configuration Tasks

The configuration includes the following tasks:

(1) Configuring the Path Cost Calculation Method

(2) Configuring the Path Cost Value

1.7.3 Configuring the Path Cost Calculation Method

1. Overview

By default, the device automatically calculates the port path cost according to the physical interface rate, and the calculation method in the specification (as shown in Table 1-11). The cost of path with high rate is low, and vice versa. This calculation method can calculate the optimal spanning tree topology.

The standard of port path cost must be unified throughout the network. The user should be able to modify the method of automatic calculation of port path cost of a device when necessary.

2. Restrictions and Guidelines

- IEEE 802.1d Short: The range of the port path cost is from 1 to 65535. Aggregate interface cost = Physical port cost × 95%.
- IEEE 802.1t Long: The range of the port path cost is from 1 to 200000000. Aggregate interface cost = Physical port cost × 95%.
- IEEE 802.1t Long Standard: The range of the port path cost is from 1 to 200000000. Aggregate interface cost = Physical port cost/Linkupcnt. At this moment, the cost value of the aggregate interface will change with the number of member ports, which will lead to the network topology change. For configurations of aggregate interfaces and the Link Aggregation Control Protocol (LACP), see *Configuring Aggregated Port*.
  - When an aggregate interface is a static aggregate interface, **Linkupcnt** refers to the number of member ports in Link Up state.
  - When an aggregate interface is an LACP aggregate interface, **Linkupcnt** refers to the number of member ports participating in the aggregate interface data forwarding.
  - When no member port of an aggregate interface 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 interface	95	1900000	2000000/Linkupcnt
100 Mbps	Common port	19	200000	200000
	Aggregate interface	18	190000	200000/Linkupcnt

Port Rate	Port	IEEE 802.1d Short	IEEE 802.1t Long	IEEE 802.1t Long Standard
1000 Mbps	Common port	4	20000	20000
	Aggregate interface	3	19000	20000/Linkupcnt
10000 Mbps	Common port	2	2000	2000
	Aggregate interface	1	1900	20000/Linkupcnt

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure port path cost.

spanning-tree pathcost method { **long** | **long standard** | **short** }

The port path cost is calculated using the long method in the IEEE 802.1t standard by default.

1.7.4 Configuring the Path Cost Value

1. Overview

In order to ignore the impact of the physical interface rate and strictly control the spanning tree calculation results, you can configure port path cost as a specified value. After configuration, the device no longer calculates the port path cost based on the physical interface rate.

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**.
- The **vlan** *vlan-list* option can be used in MVST and Rapid-MVST modes. The *vlan-list* parameter indicates a string of VLAN IDs, such as 1–10,20–30,40,50.
- **cost** *cost*: Specifies the path cost value. The value range is from 1 to 200000000. A larger value of *cost* indicates a greater path cost.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(1) Enter the global configuration mode.

configure terminal

(2) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(3) Configure the port path cost.

spanning-tree [**mst** *instance-id* | **vlan** *vlan-list*] **cost** *cost*

The port path cost is calculated based on the interface link rate by default.

1.8 Configuring Spanning Tree Time Parameters

1.8.1 Overview

The timer in STP affects the spanning tree election and recovery performance.

You can use the **spanning-tree** command to configure the following time parameters. Each configuration command can only carry one parameter. Only one of the following time parameters can be carried in the **spanning-tree** command:

- Interval for port state change (**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**)

1.8.2 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**.

1.8.3 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 the status change of a spanning tree port 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.

1.9 Configuring the Maximum Hop Count for BPDUs

1.9.1 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.

1.9.2 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**.

1.9.3 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.

1.10 Configuring Fast Convergence of Spanning Trees

1.10.1 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 1.1.4 5 Fast Convergence of RSTP.

1.10.2 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.
- You can use the **show spanning-tree** [**mst** *instance-id*] { *port-index* | **interface** *interface-type interface-number* [**link-type**] } command to view the configuration results.

1.10.3 Prerequisites

- Configure the interface as a Layer 2 interface.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure fast convergence for spanning trees.

spanning-tree link-type { **point-to-point** | **shared** }

By default, 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.

1.11 Enabling Protocol Migration

1.11.1 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 user 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

1.11.2 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*]

1.12 Configuring Spanning Tree Compatibility for Interfaces

1.12.1 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 0 (exists by default), 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.

1.12.2 Prerequisites

- Configure the interface as a Layer 2 interface.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure spanning tree compatibility for an interface.

spanning-tree compatible enable

The spanning tree compatibility function of interfaces is disabled by default.

1.13 Enabling the STP Function

1.13.1 Overview

Unless otherwise specified, STP should be enabled on each device.

1.13.2 Restrictions and Guidelines

STP and the Transparent Interconnection of Lots of Links (TRILL) protocol of data centers are mutually exclusive.

1.13.3 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.

1.14 Configuring Port Protection

1.14.1 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.

1.14.2 Restrictions and Guidelines

A device cannot be a root bridge and a non-root bridge at the same time. Therefore, root guard and loop guard cannot take effect on a port at the same time.

1.14.3 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

1.14.4 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 Layer 2 Ethernet interface configuration mode or Layer 2 aggregate port 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 Layer 2 Ethernet interface configuration mode or Layer 2 aggregate interface configuration mode to disable the root guard function and restore the port to the normal state.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Enable the root guard function.

spanning-tree guard root

The root guard function is disabled on an interface by default.

1.14.5 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

- 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, causing loops in the network. 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

- You can configure the loop guard function in the global configuration mode or interface configuration mode. Please select one configuration mode to configure this function.
- In global configuration mode, run the **spanning-tree loopguard default** command to enable the loop guard function on all Layer 2 Ethernet interface and Layer 2 aggregate interfaces, or run the **no spanning-tree loopguard default** command to disable the loop guard function of all Layer 2 Ethernet interface and Layer 2 aggregateinterfaces.
- InLayer 2 Ethernet interface and Layer 2 aggregate 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. Prerequisites

- Configure the interface as a Layer 2 interface.

4. Procedure(global configuration mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the loop guard function on all Layer 2 Ethernet interface and Layer 2 aggregate interfaces.

spanning-tree loopguard default

The loop guard function is enabled on allLayer 2 Ethernet interface and Layer 2 aggregateinterfaces by default.

5. 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.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Enable the loop guard function.

spanning-tree guard loop

The loop guard function is disabled on an interface by default.

1.15 Configuring BPDU Source MAC Address Check

1.15.1 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.

1.15.2 Restrictions and Guidelines

- In Layer 2 Ethernet interface configuration mode or Layer 2 aggregate interface configuration mode, run the **bpdu src-mac-check** *mac-address* 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.
- *mac-address* 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.

1.15.3 Prerequisites

Configure an interface as a Layer 2 interface.

1.15.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Enable BPDU source MAC address check so that only BPDUs with the source MAC address matching *mac-address* are received.

bpdu src-mac-check *mac-address*

The BPDU source MAC address check function is disabled on an interface by default.

1.16 Configuring an Edge Port

1.16.1 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**.

1.16.2 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.

- You can use the **show spanning-tree** [**mst** *instance-id*] { *port-index* | **interface** *interface-type interface-number* [**portfast**] } command to check the configuration result.

1.16.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring Autoedge
- Configuring the Port Fast Attribute

1.16.4 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

You can use the **spanning-tree autoedge disabled** command to disable the autoedge function.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the autoedge function.

spanning-tree autoedge [**disabled**]

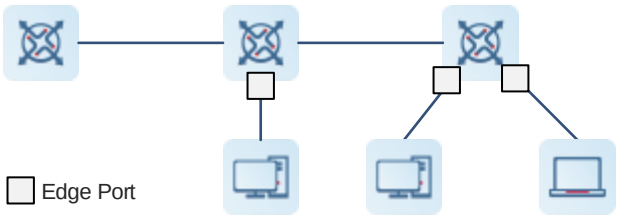
The autoedge function is enabled by default.

1.16.5 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

- Oly a Layer 2 Ethernet interface or Layer 2 aggregate interface can be configured as an edge port.
- In global configuration mode, you can use the **spanning-tree portfast default** command to configure all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces as edge ports, use the **no spanning-tree**

portfast default command to restore all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces as non-edge ports.

- In Layer 2 Ethernet interface configuration mode or Layer 2 aggregate interface configuration mode, you can use the **spanning-tree portfast** command to configure this interface as an edge port, and use the **spanning-tree portfast disabled** command to restore this interface as a non-edge port.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. ProcedureProcedure (global configuration mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.
configure terminal

- Configure all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces as edge ports.
  spanning-tree portfast default

  by default, an interface is a non-edge port.

5. 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.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure this interface as an edge port.
spanning-tree portfast

1.17 Configuring BPDU Guard or BPDU Filter

1.17.1 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.

1.17.2 Restrictions and Guidelines

BPDU guard has a higher priority than BPDU filter. If both BPDU filter and BPDU guard are enabled on an interface, only BPDU guard takes effect.

- You can use the **show spanning-tree** [**mst** *instance-id*] { *port-index* | **interface** *interface-type interface-number* [**bpdufilter** | **bpduguard**] } command to check the configuration result.

1.17.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring BPDU Guard
- Configuring BPDU Filter

1.17.4 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.

2. Restrictions and Guidelines

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.

- 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* in the *Interface Configuration Guide*.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. **Procedure** (global configuration mode)

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

- Enable the global BPDU guard function. The function takes effect only on edge ports.
  spanning-tree portfast bpduguard default

  By default, the global BPDU guard function is disabled.

5. **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.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Enable the BPDU guard function.
spanning-tree bpduguard enable

By default, the interface BPDU guard function is disabled.

1.17.5 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.

2. Restrictions and Guidelines

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.

- 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 **enable** parameter is used to enable the BPDU filter function and the **disabled** parameter is used to disable the BPDU filter function.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. **Procedure** (global configuration mode)

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

- Enable the global BPDU filter function. The function takes effect only on edge ports.
  spanning-tree portfast bpdufilter default

  By default, the global BPDU filter function is disabled.

5. **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.

- Enter the Layer 2 Ethernet interface configuration mode.
  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Configure the BPDU filter function.

- Enable the BPDU filter function.

  spanning-tree bpdufilter enable
- Disable the BPDU filter function.
  spanning-tree bpdufilter disabled

  By default, the interface BPDU filter function is disabled.

1.18 Configuring TC Attack Defense Functions

1.18.1 Overview

When the downstream network topology in port forwarding state changes (from Blocking to Forwarding, for example), 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 a Layer 3 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, TC packets generated or received by the port will not be diffused 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 Layer 3 devices, this function can effectively prevent interruption of core routes caused by access device flapping.

- 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.

1.18.2 Restrictions and Guidelines

It is recommended that the TC attack defense functions be enabled only when the network is attacked by TC packets.

1.18.3 Configuration Tasks

The configuration includes the following tasks:

- Configuring TC Protection
- Configuring TC Guard
- Configuring TC Filter

1.18.4 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 Layer 2 Ethernet interfaces and Layer 2 aggregate 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. Prerequisites

- Configure the interface as a Layer 2 interface.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable TC guard on all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

spanning-tree tc-protection

TC guard is disabled globally by default.

1.18.5 Configuring TC Guard

1. Overview

After the TC guard function is enabled, TC packets received over an interface are not flooded to other interfaces, which effectively controls TC attacks and maintains network stability.

The TC guard function is divided into global TC guard function and interface TC guard function.

- In the global configuration mode, TC guard function takes effect on all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces if enabled. In this case, all ports will not diffuse TC packets to other ports. TC guard is suitable to be enabled on desktop access devices.
- In the Layer 2 Ethernet interface configuration mode or the Layer 2 aggregate interface configuration mode, the TC guard function only takes effect on the current interface. In this case, this interface will not diffuse TC packets to other ports. TC guard is suitable to be enabled on the uplink port, especially the port connecting the aggregation switch to the core switch.

2. Restrictions and Guidelines

- In global configuration mode, run the **spanning-tree tc-protection tc-guard** command to enable the TC guard function globally, or run the **no spanning-tree tc-protection tc-guard** command to disable the TC guard function globally.
- In interface configuration mode, run the **spanning-tree tc-guard** command to enable the TC guard function on an interface, or run the **no spanning-tree tc-guard** command to disable the TC guard function on an interface.
- 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. Enabling the TC guard function will also limit the transmisson of normal TC packets. When the spanning tree network topology changes, the device cannot obtain the topology change information, and cannot clear MAC addresses in time, which may lead to packet forwarding errors. If the topology cannot be restored automatically, communication may be interrupted. Therefore, it is recommended to enable this function only when there is an illegal TC packet attack in the network.

3. Prerequisites

- Configure the interface as a Layer 2 interface.

4. **Procedure** (global configuration mode)

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

- Enable TC guard on all Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.
  spanning-tree tc-protection tc-guard

  By default, TC guard is disabled globally.

5. **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.
- Enter the Layer 2 Ethernet interface configuration mode.
interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.
interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Enable TC guard on the interface.
spanning-tree tc-guard

By default, TC guard is disabled on an interface.

1.18.6 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 Layer 2 Ethernet interface configuration mode or Layer 2 aggregate 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. Prerequisites

Configure the interface as a Layer 2 interface.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.
- Enter the Layer 2 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }
- Enter the Layer 2 aggregate interface configuration mode.

interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(4) Enable TC filter on an interface.

spanning-tree ignore tc

TC filter is disabled on an interface by default.

1.19 Configuring BPDU Tunnel

1.19.1 Overview

BPDU tunnel is a Layer 2 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 Dot1q-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 Dot1q-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*.

1.19.2 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.

1.19.3 Prerequisites

Configure the interface as a Layer 2 interface.

1.19.4 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 2 aggregate interface configuration mode.

  interface { **aggregateport** *interface-number* | **range aggregateport** *interface-range* }

(6) Enable the STP BPDU tunnel function on the interface.

l2protocol-tunnel stp enable

The STP BPDU tunnel function is disabled on the interface by default.

1.20 Configuring BPDU Transparent Transmission

1.20.1 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.

1.20.2 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.

1.20.3 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.

1.21 Configuring STP in the Specified VLAN

1.21.1 Overview

The STP function can be configured by VLAN to provide a more flexible spanning tree deployment mode and improve the spanning tree compatibility. Each VLAN can run an independent spanning tree and users can enable or disable the STP function in the specified VLAN based on actual needs to implement VLAN-based load balancing. This feature takes effect in MVST and Rapid-MVST modes. After you enable STP in the specified VLAN, if the allowed VLAN list of the interface contains this VLAN, the interface participates in spanning tree calculation in the VLAN. Otherwise, the interface does not participate in spanning tree calculation. If STP is not enabled in a VLAN, interfaces in this VLAN do not participate in the calculation but keeps the forwarding state.

1.21.2 Restrictions and Guidelines

- When you enable spanning tree by VLAN but the VLAN does not exist or the device is not in the MVST or Rapid-MVST mode, you can configure this feature. However, the configuration takes effect only when the corresponding VLAN is created and the device is switched to the MVST or Rapid-MVST mode.
- The software version must support the MVST or Rapid-MVST mode. To verify the support for MVST or Rapid-MVST, run the corresponding command to switch the spanning tree mode to MVST or Rapid-MVST.
- Before you enable spanning tree by VLAN, you are advised to switch the spanning tree mode to MVST or Rapid-MVST.
- It is recommended that trunk ports be used to connect this device to another device working in the MVST or Rapid-MVST mode. Do not use two types of ports, such as access port and trunk port.
- Interconnected devices in the spanning tree network must use the same spanning tree mode, such as STP, RSTP, MSTP, MVST, or Rapid-MVST.
- When two devices are interconnected in MVST or Rapid-MVST mode, the interconnected trunk ports must have the same native VLAN.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Switch the spanning tree mode to MVST or Rapid-MVST.

spanning-tree mode { **mvst** | **rapid-mvst** }

(4) Enable STP by VLAN.

spanning-tree vlan *vlan-list*

STP is disabled in all VLANs by default.

1.22 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.
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 vlan { *vlan-list* | **all** }	Displays the spanning tree configuration and status information of the specified VLANs.
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.

Command	Purpose
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.
clear spanning-tree mst *instance-id* **topochange record**	Clears the STP topology change information.

1.23 Configuration Examples

1.23.1 Configuring MSTP

1. Requirements

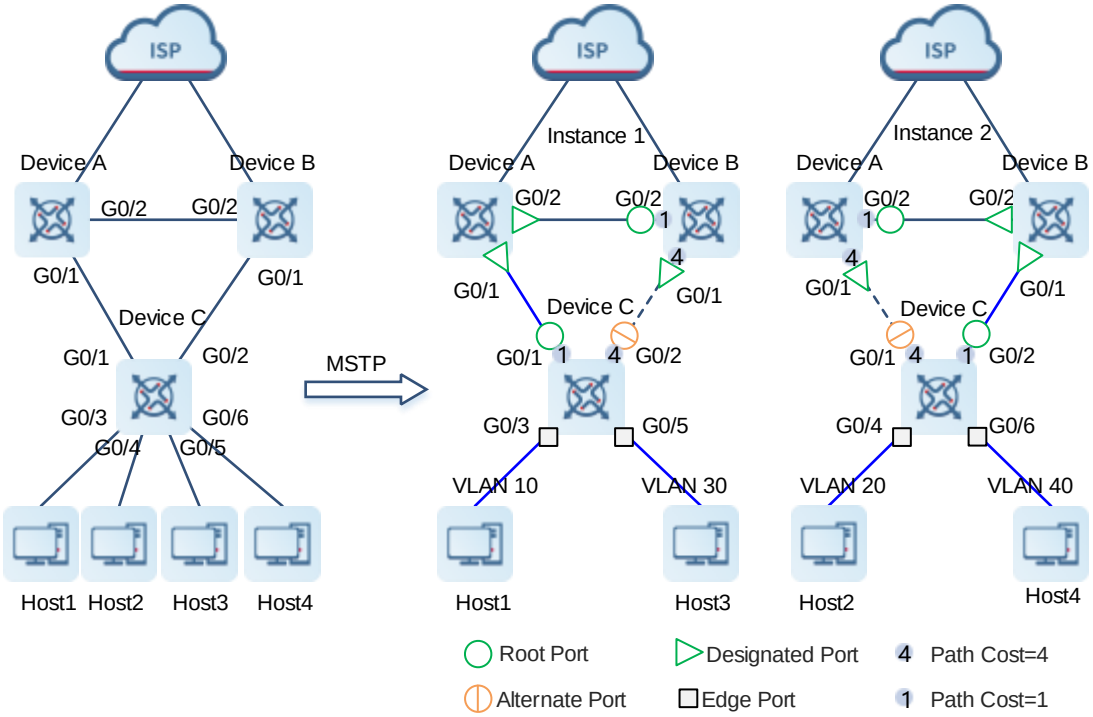
The topology shown in Figure 1-18 includes two layers: Device A and Device B are in the core layer, Device C is in the access layer, and Device C connects to intranet terminals. There are four VLANs in the intranet. The configured MSTP needs to meet the following requirements:

- 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 Topology of Configuring 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 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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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 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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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 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)# switchport trunk native vlan 1
DeviceB(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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 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)# switchport trunk native vlan 1
DeviceB(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
DeviceB(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
DeviceB(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)# switchport trunk native vlan 1
DeviceC(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
spanning-tree mst 2 cost 4
!
interface GigabitEthernet 0/2
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
spanning-tree mst 1 cost 4
spanning-tree mst 0 cost 4
!
interface GigabitEthernet 0/2
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

```
 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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
 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
switchport mode access
switchport access vlan 10
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
!
interface GigabitEthernet 0/4
switchport
switchport mode access
switchport access vlan 20
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
!
interface GigabitEthernet 0/5
switchport
switchport mode access
switchport access vlan 30
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree autoedge disabled
!
interface GigabitEthernet 0/6
switchport
switchport mode access
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.

1.23.2 Configuring MSTP+VRRP

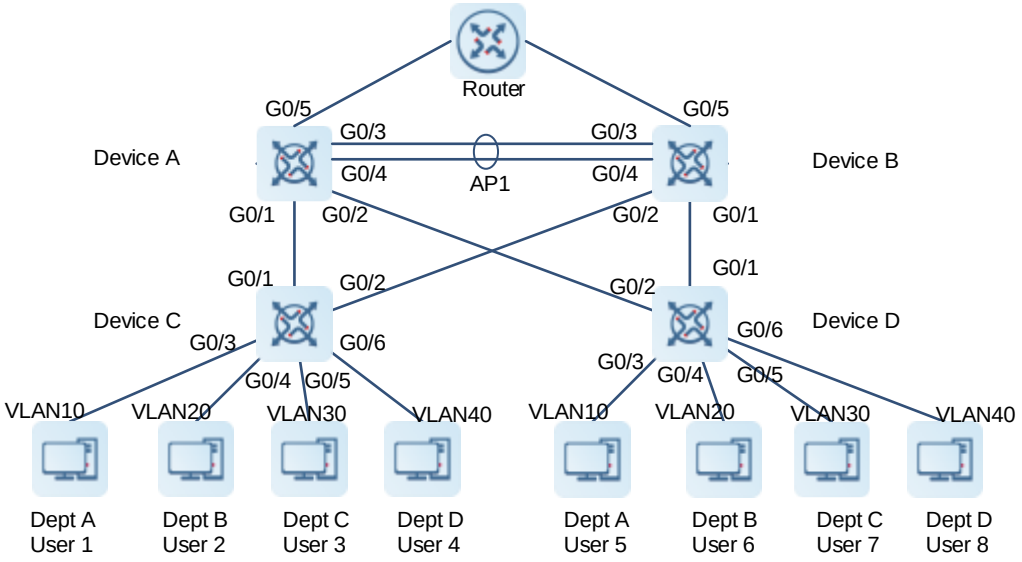
1. Requirements

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 Topology of Configuring MSTP+VRRP



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 a Layer 3 interface and configure an IP address for the port. Layer 3 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*. When the link state of the monitored interface or IP route reachability status changes, VRRP priority will change, and the change value is *decrement*. 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 Layer 3 interface 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 Layer 3 interface 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 interface 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)# interface aggregateport 1
DeviceA(config-if-AggregatePort 1)# switchport
DeviceA(config-if-AggregatePort 1)# switchport mode trunk
DeviceA(config-if-AggregatePort 1)# switchport trunk native vlan 1
DeviceA(config-if-AggregatePort 1)# switchport trunk allowed vlan all
DeviceA(config-if-AggregatePort 1)# exit
```

On Device B, configure ports GigabitEthernet 0/3 and 0/4 as AggregatePort 1 and set the aggregate interface 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)# interface aggregateport 1
DeviceB(config-if-AggregatePort 1)# switchport
DeviceB(config-if-AggregatePort 1)# switchport mode trunk
DeviceB(config-if-AggregatePort 1)# switchport trunk native vlan 1
DeviceB(config-if-AggregatePort 1)# switchport trunk allowed vlan all
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
```

```
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# switchport trunk native vlan 1
DeviceA(config-if-range)# switchport trunk allowed vlan all
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
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# switchport trunk native vlan 1
DeviceA(config-if-range)# switchport trunk allowed vlan all
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
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# switchport trunk native vlan 1
DeviceA(config-if-range)# switchport trunk allowed vlan all
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
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# switchport trunk native vlan 1
DeviceA(config-if-range)# switchport trunk allowed vlan all
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
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
DeviceC(config-if-GigabitEthernet 0/3)# 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
DeviceC(config-if-GigabitEthernet 0/3)# 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
DeviceC(config-if-GigabitEthernet 0/3)# 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
DeviceC(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
DeviceC(config-if-GigabitEthernet 0/3)# 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
DeviceC(config-if-GigabitEthernet 0/3)# 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
DeviceC(config-if-GigabitEthernet 0/3)# switchport mode access
DeviceD(config-if-GigabitEthernet 0/6)# switchport access vlan 40
DeviceD(config-if-GigabitEthernet 0/6)# end
DeviceD# write
```

5. Verification

Run the **show spanning-tree summary** command to display the spanning tree topology.

View spanning tree topology on Device A. Device A (00d0.f822.3344) is the root.

```
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
```

View spanning tree topology on Device B. Device A (00d0.f822.3344) is the root.

```
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
```

View spanning tree topology on Device C and Device D. Device C is taken as an example. Device A (00d0.f822.3344) is the root.

```
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
```

Run the **show vrrp brief** command to check whether VRRP active/standy relationship is successfully established. VLAN 10 and VLAN 30 use Device A as the master device and Device B as the standby device. VLAN 20 and VLAN 40 use Device B as the master device and Device A as the standby device.

```
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
```

Run the **show vrrp brief** command on Device B to check whether VRRP active/standy relationship is successfully established.

```
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. VLAN 10 and VLAN 30 use Device A as the master device and Device B as the standby device.

Run the **show vrrp brief** command on Device A to check VRRP status change.

```
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
```

Run the **show vrrp brief** command on Device B to check VRRP status change.

```
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. VLAN 20 and VLAN 40 use Device B as the master device and Device A as the standby device.

Run the **show vrrp brief** command on Device A to check VRRP status change.

```
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
```

Run the **show vrrp brief** command on Device B to check VRRP status change.

```
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

```
hostname DeviceA
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
 port-group 1
!
interface GigabitEthernet 0/4
 port-group 1
!
interface AggregatePort 1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
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

```
hostname DeviceB
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
 port-group 1
!
interface GigabitEthernet 0/4
```

```
 port-group 1
!
interface AggregatePort 1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

```
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
switchport
switchport mode access
switchport access vlan 10
 spanning-tree bpduguard enable
 spanning-tree portfast
!
interface GigabitEthernet 0/4
switchport
switchport mode access
switchport access vlan 20
 spanning-tree bpduguard enable
 spanning-tree portfast
!
interface GigabitEthernet 0/5
switchport
switchport mode access
switchport access vlan 30
 spanning-tree bpduguard enable
 spanning-tree portfast
!
interface GigabitEthernet 0/6
switchport
switchport mode access
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.

1.23.3 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 Topology of Spanning Tree Compatibility for MSTP Interfaces

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
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode access
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
```

```
DeviceA(config-if-GigabitEthernet 0/2)# switchport mode access
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
switchport mode access
 switchport access vlan 10
spanning-tree compatible enable
!
interface GigabitEthernet 0/2
switchport
switchport mode access
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.

1.23.4 Configuring BPDU Tunnel

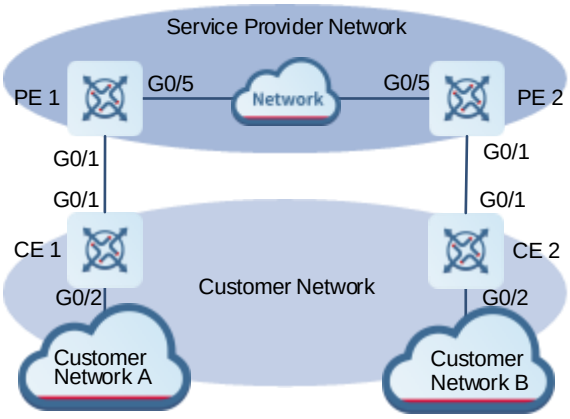
1. Requirements

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 a Layer 2 protocol tunnel to transparently transmit Layer 2 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 Topology of Configuring BPDU Tunnel



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 Dot1q-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 Dot1q-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)# switchport trunk native vlan 1
PE1(config-if-GigabitEthernet 0/5)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
CE1(config-if-range)# switchport trunk allowed vlan all
CE1(config-if-range)# end
CE1# write
```

5. Verification

(1) Check Dot1q-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
 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
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- 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
 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
switchport mode uplink
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- 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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- CE 2 configuration file

```
spanning-tree mode stp
spanning-tree
!
sysmac 0074.9c11.c9e6
!
interface GigabitEthernet 0/1
switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
```

```
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

7. Common Errors

- The Layer 2 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.

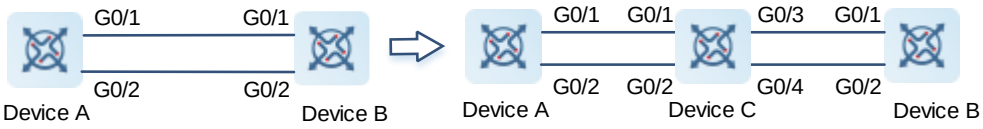
1.23.5 Configuring BPDU Transparent Transmission

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 Topology of 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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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)# switchport trunk native vlan 1
DeviceA(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
DeviceA(config-if-GigabitEthernet 0/2)# spanning-tree mst 0 port-priority 16
DeviceA(config-if-GigabitEthernet 0/2)# exit
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)# switchport trunk native vlan 1
DeviceB(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan all
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
DeviceB(config-if-GigabitEthernet 0/2)# switchport trunk native vlan 1
DeviceB(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan all
```

(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
DeviceC(config-if-rang)# switchport trunk native vlan 1
DeviceC(config-if-rang)# switchport trunk allowed vlan all
```

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
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
spanning-tree mst 0 port-priority 16
```

- Device B configuration file

```
spanning-tree

interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

- Device C configuration file

```
bridge-frame forwarding protocol bpdu
!
interface GigabitEthernet 0/1
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/2
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/3
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
!
interface GigabitEthernet 0/4
 switchport
switchport mode trunk
switchport trunk native vlan 1
switchport trunk allowed vlan only 1-4094
```

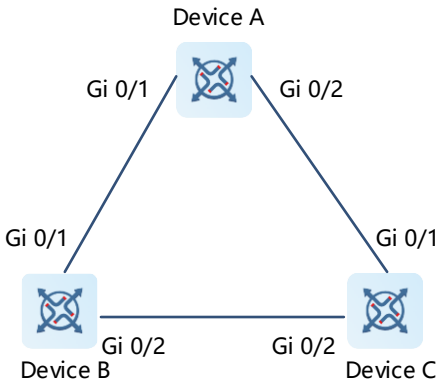
1.23.6 Configuring MVST

1. Requirements

As shown in Figure 1-18, Device A, Device B, and Device C form a loop topology. All the three devices must support MVST.

2. Topology

Figure 1-4 MVST Topology



3. Procedure

(1) Configure MVST on Device A.

Create VLANs 1–3 and configure the interfaces connecting to other devices as trunk interfaces.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan rang 1-3
DeviceA(config-vlan-range)# exit
DeviceA(config)# interface range gigabitethernet 0/1-2
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode trunk
```

Set the spanning tree mode to MVST, enable the STP function in VLANs 1–3, set the global bridge priority to 0 in VLANs 1–3, and then enable the STP function globally.

```
DeviceA(config)# spanning-tree mode mvst
DeviceA(config)# spanning-tree vlan 1-3
DeviceA(config)# spanning-tree vlan 1-3 priority 0
DeviceA(config)# spanning-tree
```

(2) Configure MVST on Device B.

Create VLANs 1–3 and configure the interfaces connecting to other devices as trunk interfaces.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan rang 1-3
DeviceB(config-vlan-range)# exit
DeviceB(config)# interface range gigabitethernet 0/1-2
```

```
DeviceB(config-if-range)# switchport
DeviceB(config-if-range)# switchport mode trunk
```

Set the spanning tree mode to MVST, enable the STP function in VLANs 1–3, set the global bridge priority to 12288 in VLANs 1–3, and then enable the STP function globally.

```
DeviceB(config)# spanning-tree mode mvst
DeviceB(config)# spanning-tree vlan 1-3
DeviceB(config)# spanning-tree vlan 1-3 priority 12288
DeviceB(config)# spanning-tree
```

(3) Configure MVST on Device C.

Create VLANs 1–3 and configure the interfaces connecting to other devices as trunk interfaces.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# vlan rang 1-3
DeviceC(config-vlan-range)# exit
DeviceC(config)# interface range gigabitethernet 0/1-2
DeviceC(config-if-range)# switchport
DeviceC(config-if-range)# switchport mode trunk
```

Set the spanning tree mode to MVST, enable the STP function in VLANs 1–3, and then enable the STP function globally.

```
DeviceC(config)# spanning-tree mode mvst
DeviceC(config)# spanning-tree vlan 1-3
DeviceC(config)# spanning-tree
```

4. Verification

(1) Run the **show spanning-tree vlan all** command to display the spanning tree status of all VLANs with MVST enabled.

Check whether the MVST configuration takes effect on Device A. In VLANs 1–3, Device A (c470.abe1.8856) is the root. In VLANs 1–3, GigabitEthernet 0/1 and GigabitEthernet 0/2 on Device A are designated ports (Desg) in Forwarding (FWD) state.

```
DeviceA# show spanning-tree vlan all

Spanning tree enabled protocol stp
VLAN 1 :
 Root ID    Priority    0
            System ID extension   1
            Address     c470.abe1.8856
            this bridge is root
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

 Bridge ID  Priority    0
            System ID extension   1
            Address     c470.abe1.8856
            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

VLAN 2 :
  Root ID    Priority    0
           System ID extension    2
           Address    c470.abe1.8856
           this bridge is root
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    0
           System ID extension    2
           Address    c470.abe1.8856
           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

VLAN 3 :
  Root ID    Priority    0
           System ID extension    3
           Address    c470.abe1.8856
           this bridge is Desg
           Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    0
           System ID extension    3
           Address    c470.abe1.8856
           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
```

Check whether the MVST configuration takes effect on Device B. In VLANs 1–3, Device A (c470.abe1.8856) is the root. In VLANs 1–3, GigabitEthernet 0/1 on Device B is root port (Root) in Forwarding (FWD) state and GigabitEthernet 0/2 on Device B is designated port (Desg) in Forwarding (FWD) state.

```
DeviceB# show spanning-tree vlan all

Spanning tree enabled protocol stp
VLAN 1 :
  Root ID    Priority    0
```

```
          System ID extension   1
          Address    c470.abe1.8856
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority   12288
          System ID extension   1
          Address    c470.abe1.8860
          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          Desg FWD 20000     128     False    P2p

VLAN 2 :
  Root ID   Priority   0
          System ID extension   2
          Address    c470.abe1.8856
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority   12288
          System ID extension   2
          Address    c470.abe1.8860
          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          Desg FWD 20000     128     False    P2p

VLAN 3 :
  Root ID   Priority   0
          System ID extension   3
          Address    c470.abe1.8856
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority   12288
          System ID extension   3
          Address    c470.abe1.8860
          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          Desg FWD 20000     128     False    P2p
```

Check whether the MVST configuration takes effect on Device C. In VLANs 1–3, Device A (c470.abe1.8856) is the root. In VLANs 1–3, GigabitEthernet 0/1 on Device C is root port (Root) in Forwarding (FWD) state and GigabitEthernet 0/2 on Device C is alternate port (Altn) in Blocking (BLK) state.

```
DeviceC# show spanning-tree vlan all

Spanning tree enabled protocol stp
VLAN 1 :
  Root ID    Priority    0
             System ID extension    1
             Address     c470.abe1.8856
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             System ID extension    1
             Address     c470.abe1.8862
             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

VLAN 2 :
  Root ID    Priority    0
             System ID extension    2
             Address     c470.abe1.8856
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             System ID extension    2
             Address     c470.abe1.8862
             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

VLAN 3 :
  Root ID    Priority    0
             System ID extension    3
```

```
          Address    c470.abe1.8856
          this bridge is root
          Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

 Bridge ID  Priority    32768
          System ID extension   3
          Address    c470.abe1.8862
          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
```

5. Configuration Files

- Device A configuration file

```
hostname DeviceA
spanning-tree mode mvst
spanning-tree vlan 1-3
spanning-tree vlan 1-3 priority 0
spanning-tree
vlan range 1-3
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode trunk
!
```

- Device B configuration file

```
hostname DeviceB
spanning-tree mode mvst
spanning-tree vlan 1-3
spanning-tree vlan 1-3 priority 12288
spanning-tree
vlan range 1-3
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode trunk
!
```

- Device C configuration file

```
hostname DeviceC
spanning-tree mode mvst
```

```
spanning-tree vlan 1-3
spanning-tree
vlan range 1-3
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode trunk
!
```

6. Common Errors

- The spanning tree function can be enabled in a VLAN before the VLAN is created. If the interface does not participate in MVST calculation, check whether the VLAN is created.
- If two devices are interconnected using MVST, the interconnected interfaces must work in the same mode. If the interfaces work in different modes, such as access port and trunk port, an error may occur during spanning tree calculation.
- Interconnected devices in the spanning tree network use different spanning tree modes, such as STP, RSTP, MSTP, MVST, or Rapid-MVST, so the spanning tree calculation result does not meet the expectations.

  When two devices are interconnected in MVST or Rapid-MVST mode, the interconnected trunk ports cannot use different native VLANs.

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 Prerequisites 8
1.4.4 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 13
1.13.1 Configuring Single-Ring Protection 13
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 Layer 2 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 Layer 2 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.

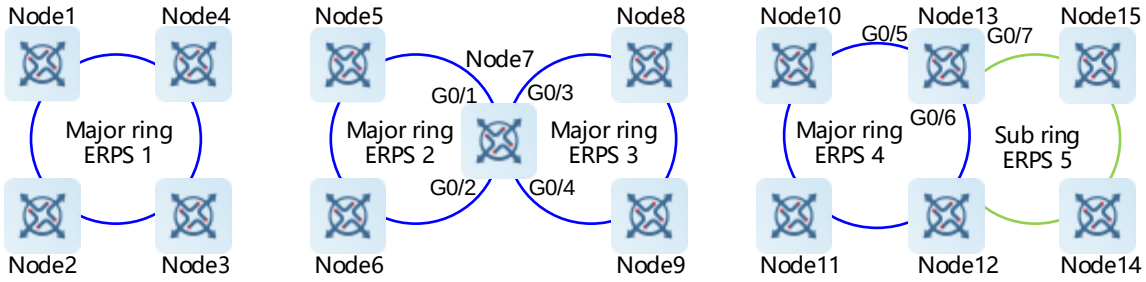
1.1.3 Basic Model of an Ethernet Ring

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 interfaces 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 interfaces 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 interfaces 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 interfaces 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 interfaces 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.

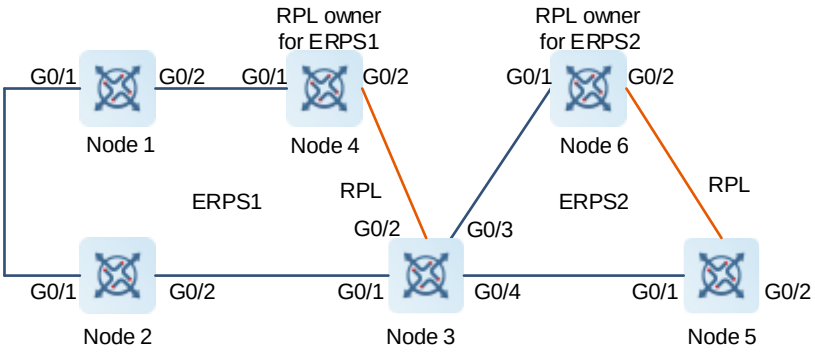
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in Figure 1-2 are RPLs, the link 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.

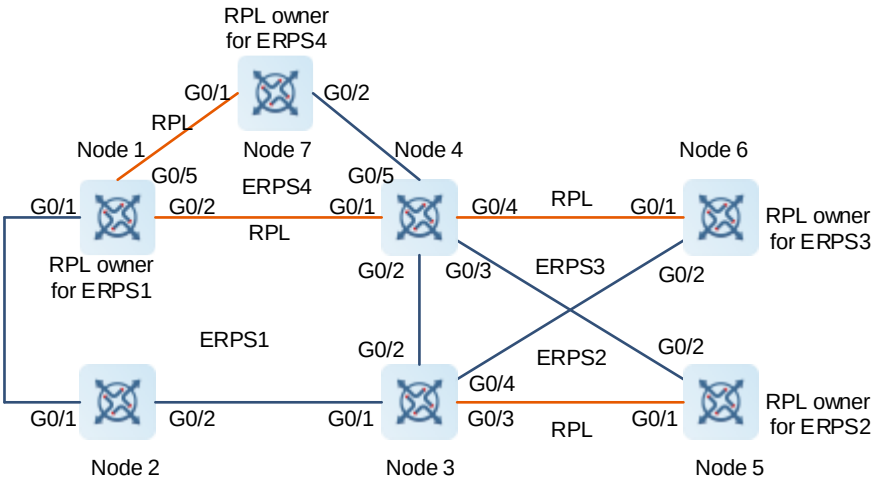
Blocked ports on RPLs are RPL ports, and RPL ports do not forward data packets to prevent loops. RPL ports are on RPL owner nodes, and the RPL owner nodes block the RPL ports. Each Ethernet ring has only one RPL owner node.

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.

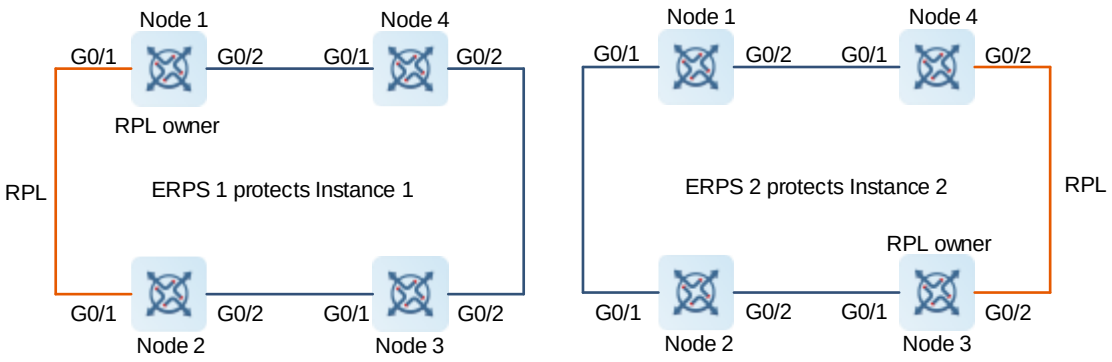
- After receiving this NR-RB packet, other nodes update their MAC address entries and ARP/ND entries, and the node that sends the NR packet stops sending the NR packet and enables the blocked ports.
- The ring network is restored to the normal state.

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, and enter the R-APS VLAN configuration mode.

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 interfaces 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 interfaces 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

- Only Trunk, Uplink or Hybrid ports can join the ERPS ring. Only a Layer 2 Ethernet interface or Layer 2 aggregate interface can be configured as Trunk, Uplink, or Hybrid port and join the ERPS ring.
- If an Ethernet ring (major or subring) passes through two interfaces on a node, run the **ring-port west** *interface-type interface-number-1* **east** *interface-type interface-number-2* command to add the two interfaces 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.
- 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 Prerequisites

(1) Configure the interface as a Layer 2 interface.

- Configure the mode of the Layer 2 interface as Trunk, Uplink or Hybrid.

1.4.4 Procedure

(1) Configure interfaces as trunk ports.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

(2) Enter the R-APS VLAN configuration mode of an Ethernet ring.

erps raps-vlan *vlan-id*

By default, an Ethernet ring control VLAN does not exist.

(3) Configure the Layer 2 Ethernet interface or Layer 2 aggregate interface as a member port of 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 Ethernet 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*

By default, an Ethernet ring control VLAN does not exist.

(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 R-APS control VLAN configuration mode of a major ring.

erps raps-vlan *major-ring-vlan-id*

(4) Associate the major ring with all subrings.

associate sub-ring raps-vlan *sub-ring-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 R-APS control VLAN configuration mode of a subring.

erps raps-vlan *sub-ring-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.

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 R-APS control VLAN configuration mode of an Ethernet ring.

erps raps-vlan *vlan-id*

By default, an Ethernet ring control VLAN does not exist.

(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 Ethernet ring control 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.

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

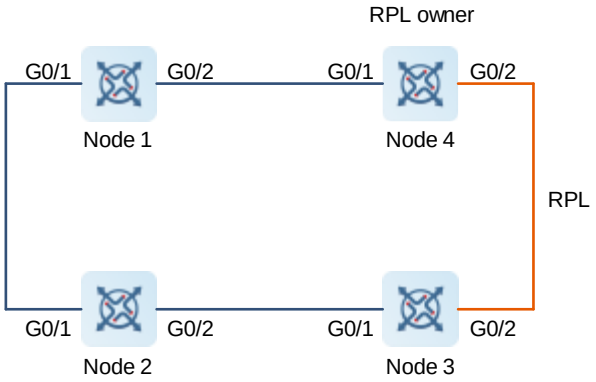
1.13.1 Configuring Single-Ring Protection

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 Topology of Configuring 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 interfaces 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 interfaces 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 interfaces 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
Node4(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 interfaces 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.

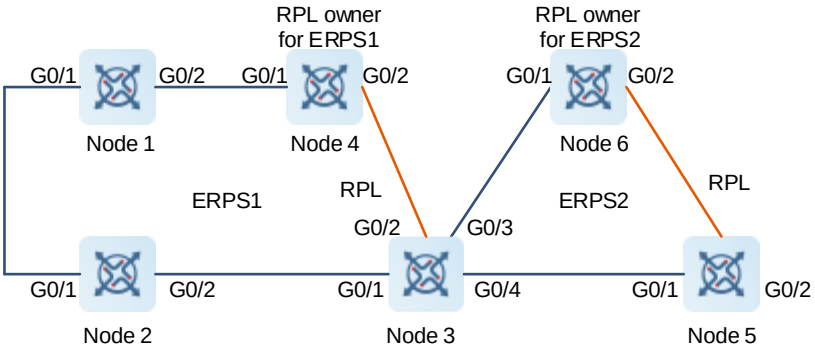
1.13.2 Configuring Tangent-Ring Protection

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 Topology of Configuring 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 interfaces 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
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 interfaces 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
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 interfaces 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
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 interfaces 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
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
```

```
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 interfaces 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
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
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 interfaces 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

- The Ethernet ring ERPS function is enabled, but the global ERPS function is not enabled. In this case, the ERPS function does not take effect. 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.

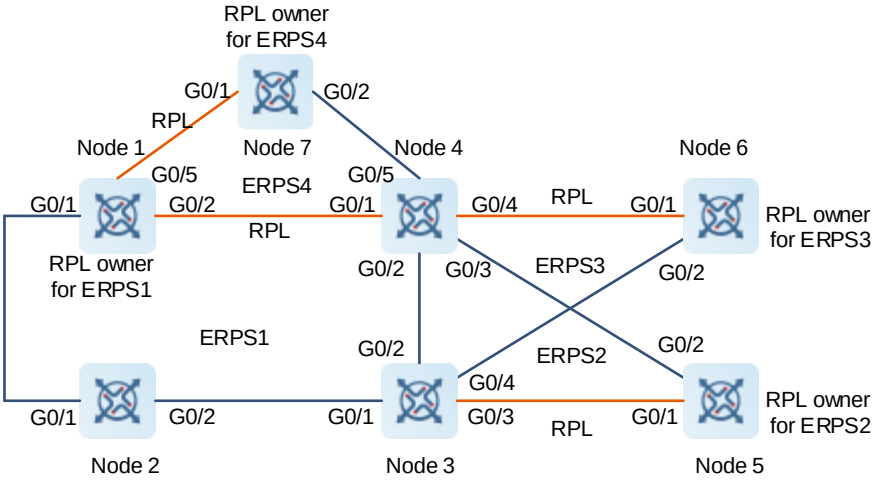
1.13.3 Configuring Intersecting-Ring Protection

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 Topology of Configuring 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 interfaces 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
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)# 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 interfaces to the Ethernet ring, and enable the ERPS function.

```
Node1(config)# interface rang gigabitethernet 0/5
Node1(config-if-range)# switchport
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 interfaces 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
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 interfaces 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
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 interfaces to the subring, and enable the ERPS function.

```
Node3(config)# interface gigabitethernet 0/3
Node3(config-if-GigabitEthernet 0/3)# switchport
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 interfaces to the subring, and enable the ERPS function.

```
Node3(config)# interface gigabitethernet 0/4
Node3(config-if-GigabitEthernet 0/4)# switchport
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 interfaces 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
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 interfaces to the subring, and enable the ERPS function.

```
Node4(config)# interface gigabitethernet 0/3
Node4(config-if-GigabitEthernet 0/3)# switchport
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 interfaces to the subring, and enable the ERPS function.

```
Node4(config)# interface gigabitethernet 0/4
Node4(config-if-GigabitEthernet 0/4)# switchport
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 interfaces to the subring, and enable the ERPS function.

```
Node4(config)# interface gigabitethernet 0/5
Node4(config-if-GigabitEthernet 0/5)# switchport
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 interfaces 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
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 interfaces 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
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 interfaces 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
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

- The Ethernet ring ERPS function is enabled, but the global ERPS function is not enabled. In this case, the ERPS function does not take effect.
- 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.

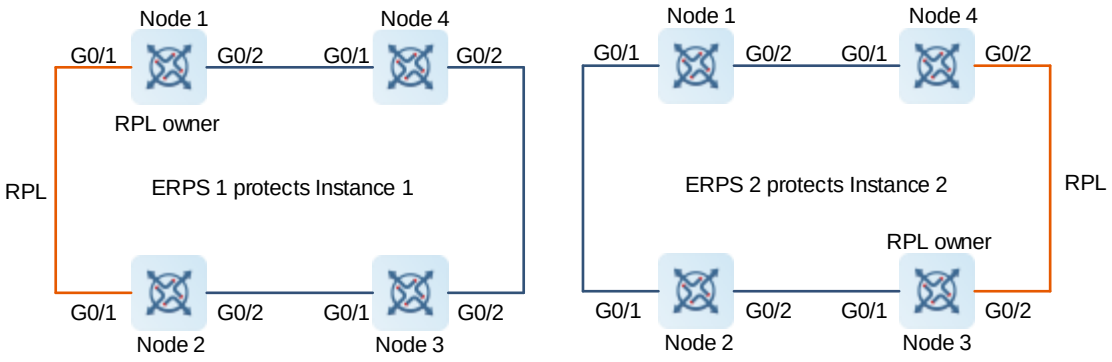
1.13.4 Configuring Load Balancing

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 Topology of Configuring 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 interfaces 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 interfaces 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 interfaces 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 interfaces 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 interfaces 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 interfaces 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
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
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
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
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

- The Ethernet ring ERPS function is enabled, but the global ERPS function is not enabled. In this case, the ERPS function does not take effect.
- Multiple RPL owner nodes are configured in one ERPS ring.
- Different R-APS VLANs are configured for the nodes in one ERPS ring.

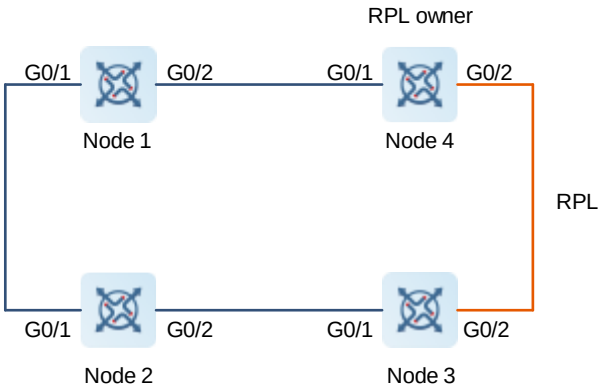
1.13.5 Modifying ERPS Configuration

1. Requirements

ERPS has been configured in an Ethernet ring. An ERPS port needs to be changed because of a physical topology change.

2. Topology

Figure 1-9 Topology 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 configuration 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 Layer 2 Ethernet 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
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 LLDPDU 2
1.1.4 TLV 3
1.1.5 LLDP Packet Transmission Mechanism 6
1.1.6 LLDP Packet Receiving Mechanism 6
1.1.7 Protocols and Standards 7
1.2 Restrictions and Guidelines 7
1.3 Configuration Task Summary 7
1.4 Enabling the LLDP Function 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 8
1.4.3 Procedure 8
1.5 Configuring the LLDP Packet Encapsulation Format 8
1.5.1 Overview 8
1.5.2 Procedure 9
1.6 Configuring LLDP Work Mode 9
1.6.1 Overview 9
1.6.2 Restrictions and Guidelines 9
1.6.3 Procedure 10

1.7 Configuring Interface Initialization Delay Time 10
1.7.1 Overview 10
1.7.2 Procedure 10
1.8 Configuring Packet Sending Interval 10
1.8.1 Overview 10
1.8.2 Restrictions and Guidelines 10
1.8.3 Procedure 11
1.9 Configuring TTL Multiplier 11
1.9.1 Overview 11
1.9.2 Restrictions and Guidelines 11
1.9.3 Procedure 11
1.10 Configuring LLDP Packet Sending Delay Time 11
1.10.1 Overview 11
1.10.2 Restrictions and Guidelines 12
1.10.3 Procedure 12
1.11 Configuring LLDP Packets Fast Sending Count 12
1.11.1 Overview 12
1.11.2 Procedure 12
1.12 Configuring LLDP Management Address 12
1.12.1 Overview 12
1.12.2 Restrictions and Guidelines 13
1.12.3 Procedure 13
1.13 Configuring Optional TLVs that an Interface can Publish 13
1.13.1 Overview 13

1.13.2 Restrictions and Guidelines 14
1.13.3 Procedure 15
1.14 Configuring Interface to Publish City Location 16
1.14.1 Overview 16
1.14.2 Restrictions and Guidelines 16
1.14.3 Procedure 17
1.15 Configuring Interface to Publish Emergency Contact Number 18
1.15.1 Overview 18
1.15.2 Restrictions and Guidelines 18
1.15.3 Procedure 18
1.16 Configuring Interface to Publish Network Policy TLV 19
1.16.1 Overview 19
1.16.2 Restrictions and Guidelines 19
1.16.3 Procedure 20
1.17 Configuring the Device to Ignore PVID Detection 21
1.17.1 Overview 21
1.17.2 Procedure 21
1.18 Configuring Compatibility with Competitor Device Discovery 21
1.18.1 Overview 21
1.18.2 Procedure 22
1.19 Configuring LLDP Alarm Function 22
1.19.1 Overview 22
1.19.2 Procedure 22
1.20 Configuring LLDP Error Detection Function 23

1.20.1 Overview 23
1.20.2 Restrictions and Guidelines 23
1.20.3 Procedure 23
1.21 Monitoring 23
1.22 Configuration Examples 24
1.22.1 Checking the Neighbors Connected to the Device by Using the LLDP Function 24
1.22.2 Configuring the LLDP Error Detection Function 26

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 to neighbors its own information by sending LLDP packets, and obtains the information of neighbors by receiving LLDP packets. LLDP packets can be encapsulated in two formats: Ethernet II and SNAP (Sub Network Access Protocols). Figure 1-1shows the format of an LLDP packet encapsulated in Ethernet frame format.

Figure 1-1 LLDP Packet Encapsulated in Ethernet Frame Format

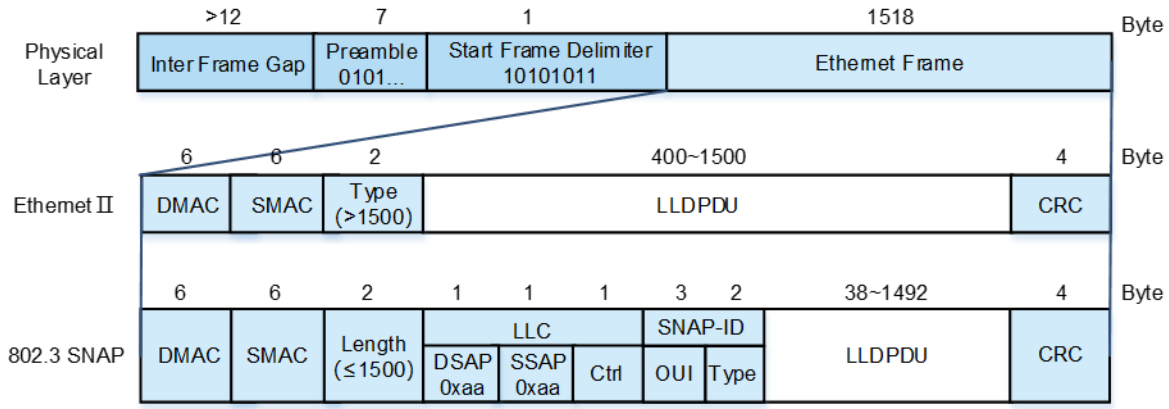


Table 1-1 describes the related fields of an LLDP packet encapsulated in Ethernet II format.

Table 1-1 Description of Fields in an LLDP Packet Encapsulated in Ethernet II Format

Field	Byte	Description
DMAC	6	Destination Address, which is a fixed multicast address 0180.c200.000e.
SMAC	6	Source Address, which is the MAC address of the device's interface.

Field	Byte	Description
Type	2	Ethernet type, which is 0x88CC.
LLDPDU	400-1500	LLDP data unit.
CRC	4	Frame check sequence.

Table 1-2 describes the related fields of an LLDP packet encapsulated in SNAP format.

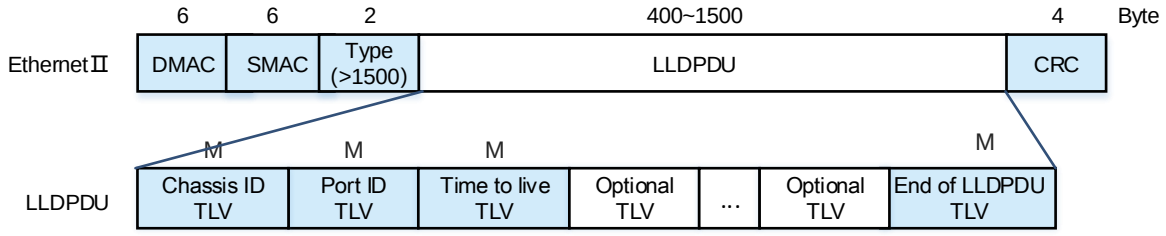
Table 1-2 Description of Fields in an LLDP Packet Encapsulated in SNAP Format

Field	Byte	Description
DMAC	6	Destination Address, which is a fixed multicast address 0180.c200.000e.
SMAC	6	Source Address, which is the MAC address of the device's interface.
DSAP	1	Destination Service Access Point. The value is 0xaa.
SSAP	1	Source Service Access Point. The value is 0xaa.
Control	1	Control information, for storing various control information and identify the type of frame. The value is 0x03.
OUI	3	Organizationally Unique Identifier, for distinguishing between basic management TLVs and TLVs defined by different organizations.
Type	2	Ethernet type, which is 0x88CC.
LLDPDU	38-1492	LLDP data unit.
CRC	4	Frame check sequence.

1.1.3 LLDPDU

The data unit in the LLDP packet is called LLDPDU (short for Link Layer Discovery Protocol Data Unit). According to the LLDP, each LLDPDU can contain 28 TLVs, starting from the Mandatory TLV - Chassis ID TLV, Port ID TLV and Time To Live TLV, Optional TLV in the middle, and LLDPDU TLV at the end. **Figure 1-2**shows the format of LLDPDU, where M represents the mandatory TLV.

Figure 1-2 Format of LLDPDU



1.1.4 TLV

The data unit field in the LLDP frame is LLDPDU, which is composed of a series of variable length information elements. Each information element is called a TLV. The device supporting LLDP function records the status information of the device to the TLV to and advertise it to the neighbor, and obtains the status information of the neighbor through the TLV.

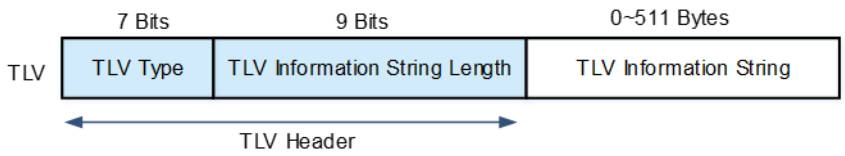
TLVs encapsulated in LLDPDUs are classified into basic management TLVs and organizationally specific TLVs.

Organizationally specific TLVs are defined by standard organizations or 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.

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.

Figure 1-3shows the structure of a TLV.

Figure 1-3 Structure of a TLV



- TLV Type: TLV type number. Different organizations advertise private information of devices by defining specific TLV types, and different TLV types are represented by numerical numbers in the TLV packet. Different organizations may define the same TLV Type number, so it is necessary to distinguish TLVs of different organizations based on the OUI (Organizationally Unique Identifier) field in the LLDP packet, and determine the TLV type based on the TLV Type value.
- TLV Information String Length: The length of TLV information. The 9-bit binary number can represent 0-511 bytes, so the length of TLV information is 0-511 bytes.
- TLV Information String: TLV information value.

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
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. 802.1 TLV

- Table 1-4 describes IEEE 802.1 organizationally specific TLVs. All TLV types are optional.

Table 1-4 IEEE 802.1 Organizationally Specific TLVs

TLV Type	Description
Port VLAN ID TLV	TLV Type is 1. Virtual local area network (VLAN) identifier of an interface.
Port And Protocol VLAN ID TLV	TLV Type is 2. Protocol VLAN identifier of an interface.
VLAN Name TLV	TLV Type is 3. VLAN name of an interface.
Protocol Identity TLV	TLV Type is 4. Protocol type supported by an interface.

Note

This LLDP-compliant device does not send the protocol identity TLV but receives this TLV.

3. 802.3 TLV

- Table 1-5 describes IEEE 802.3 organizationally specific TLVs. All TLV types are optional.

Table 1-5 IEEE 802.3 Organizationally Specific TLVs

TLV Type	Description

TLV Type	Description
MAC/PHY Configuration//Status TLV	TLV Type is 1. Rate and duplex mode of an interface, and whether auto-negotiation is supported and enabled.
Power Via MDI TLV	TLV Type is 2. Power supply capacity of an interface.
Link Aggregation TLV	TLV Type is 3. Link aggregation capacity of an interface and the current aggregation state.
Maximum Frame Size TLV	TLV Type is 4. 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 (Link Layer Discovery Protocol-Media Endpoint Discovery) 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. All TLV types are optional.

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	Contains city location (common address and device type) and emergency contact number, which can be used to accurately locate endpoint devices in applications such as network topology collection.
Extended Power-via-MDI TLV	Extended power supply capacity.
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.

TLV Type	Description
Inventory – Manufacturer Name TLV	Name of the manufacturer of a MED device.
Inventory – Model Name TLV	Module name of a MED device.
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.

1.1.5 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 supports three work modes.

- TxRx: Transmits and receives LLDPDUs.
- Rx Only: Only receives LLDPDUs.
- Tx Only: Only transmits LLDPDUs.

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 Restrictions and Guidelines

- LLDP can only be enabled on a physical interface, including Layer 2 Ethernet interface, Layer 3 Ethernet interface.
- For the aggregate interface, LLDP can be enabled on the member ports of the aggregate interface. The stack port and VSL (Virtual Switching Link) port also do not support LLDP.

1.3 Configuration Task Summary

The following tasks are optional:

(1) Enabling the LLDP Function

(2) Configuring the LLDP Transmission Mechanism

- Configuring the LLDP Packet Encapsulation Format
- Configuring LLDP Work Mode

(3) Configuring LLDP performance parameters

- Configuring Interface Initialization Delay Time
- Configuring Packet Sending Interval
- Configuring TTL Multiplier
- Configuring LLDP Packet Sending Delay Time
- Configuring LLDP Packets Fast Sending Count

(4) Configuring TLV Published in LLDPDU

- Configuring LLDP Management Address
- Configuring Optional TLVs that an Interface can Publish
- Configuring Interface to Publish City Location
- Configuring Interface to Publish Emergency Contact Number
- Configuring Interface to Publish Network Policy TLV

(5) Configuring the Device to Ignore PVID Detection

(6) Configuring Compatibility with Competitor Device Discovery

(7) Configuring LLDP Alarm Function

(8) Configuring LLDP Error Detection Function

1.4 Enabling the LLDP Function

1.4.1 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.

1.4.2 Restrictions and Guidelines

- You can enable the LLDP function on a Layer 2 Ethernet interface, Layer 3 Ethernet interface.
- To make the LLDP function take effect on an interface, the LLDP function must be enabled globally and on the interface.
- You can run the **lldp enable** command in global configuration mode to enable the LLDP function globally, and run the **lldp enable** command in interface configuration mode to enable LLDP function on an interface.
- LLDP function is enabled by default. You can use the **no lldp enable** command 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.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the LLDP function globally.

lldp enable

The global LLDP function is enabled by default.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(5) Enable the LLDP function on the interface.

lldp enable

The LLDP function is enabled on interfaces by default.

1.5 Configuring the LLDP Packet Encapsulation Format

1.5.1 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.

You can use the **no lldp encapsulation snap** command to configure the LLDP packet encapsulation format as SNAP, or use the **no lldp encapsulation snap** command to restore the packet encapsulation format to Ethernet II.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(4) Set the LLDP packet encapsulation format to SNAP.

lldp encapsulation snap

The default LLDP packet encapsulation format is Ethernet II.

1.6 Configuring LLDP Work Mode

1.6.1 Overview

LLDP supports three work modes. This device has a default configuration, and configuration commands of this function are optional.

- TxRx: Transmits and receives LLDPDUs.
- Rx Only: Only receives LLDPDUs.
- Tx Only: Only transmits LLDPDUs.

When the LLDP work mode of the interface changes, the interface will initialize the protocol state machine. To avoid frequent initialization of the state machine caused by frequent changes in the interface work mode, the delay time of interface initialization can be configured in the global configuration mode.

1.6.2 Restrictions and Guidelines

- By default, the work mode of LLDP is **txrx**, indicating that the interface sends and receives LLDPDU. You can configure the work mode as **tx** or **rx** according to actual needs.
- When the LLDP work mode of the interface is **tx**, the interface can only send packets but not receive packets.
- When the LLDP work mode of the interface is **rx**, the interface can only receive packets but not send packets.

You can use the **no lldp mode** command to disable LLDP work mode of the interface, and the interface will not send or receive LLDP packets.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(4) Configure the LLDP work mode.

lldp mode { **rx** | **tx** | **txrx** }

By default, the LLDP work mode is sending and receiving LLDPDU.

1.7 Configuring Interface Initialization Delay Time

1.7.1 Overview

To avoid frequent initialization of the state machine caused by frequent changes in the interface work mode, the delay time of interface initialization can be configured in the global configuration mode.

1.7.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the interface initialization delay time.

lldp timer reinit-delay *reinit-delay*

By default, the LLDP interface initialization delay time is 2 seconds.

1.8 Configuring Packet Sending Interval

1.8.1 Overview

The time interval for sending LLDP packet refers to the period for sending LLDP packet. A short period indicates high LLDP transmission frequency, increasing the system resource consumption. If the period is too long, the peer device may not discover the local device in time. According to the actual needs of the network, the time interval for sending LLDP packets can be configured to change the network topology discovery frequency.

1.8.2 Restrictions and Guidelines

- For standard MIB, the sending interval of LLDP packet is 5-32768 seconds.

- The value range of *tx-interval* is 1-32768, in seconds. The range is larger than that of the standard MIB to meet the requirements of more scenarios.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the sending interval of LLDP packets.

lldp timer tx-interval *tx-interval*

By default, the LLDP packet sending interval is 30 seconds.

1.9 Configuring TTL Multiplier

1.9.1 Overview

In the LLDP packet, TLV indicates the lifetime of the device's information on the neighbor device.

Time To Live TLV = TTL Multiplier × Packet Sending Interval + 1. TLV value can be modified by configuring TTL multiplier and LLDP packet sending interval. For example, if the TTL multiplier is 2, and the packet sending interval is 30 seconds, then the time to live of the LLDP packet of this device on the neighbor device is 2 × 30+1=61 seconds.

1.9.2 Restrictions and Guidelines

- You can use the **lldp hold-multiplier** *ttl-value* command to adjust the TTL multiplier in order to control the time to live of the device information on the neighbor device.

1.9.3 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*

By default, the TTL multiplier of LLDP packet is 4.

1.10 Configuring LLDP Packet Sending Delay Time

1.10.1 Overview

When the status information of a local device changes, the local device will send a LLDP packet to neighbor devices immediately. To avoid frequently sending LLDP packets caused by frequent changes in local status information, you can configure the LLDP packet sending delay time to restrict the frequent sending of LLDP packets.

1.10.2 Restrictions and Guidelines

- The LLDP packet sending delay time is 2 seconds by default. *tx-delay* is the LLDP packet sending delay time configuration parameter, with a value range of 1-8192 seconds.
- If the value of delay time is too small, LLDP packets will be frequently sent due to the change of local status information. If the value of delay time is too large, the LLDP packet cannot be sent in time after a change occurred in the local status information. You are advised to configure the delay time according to the actual situation.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the LLDP packet sending delay time.

lldp timer tx-delay *tx-delay*

By default, the LLDP packet sending delay time is 2 seconds.

1.11 Configuring LLDP Packets Fast Sending Count

1.11.1 Overview

When a new neighbor is discovered, or the LLDP work mode is changed from Disabled or Rx to TxRx or Tx, the device will start the fast sending mechanism to enable the neighbor device to learn the information of the device as soon as possible. The fast sending mechanism will shorten the sending period of LLDP packet to 1 second, and continuously send a certain number of LLDP packets, and then resume the normal sending interval. You can use this function to configure the number of LLDP packets sent under the fast sending mechanism.

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the fast sending count of LLDP packets.

lldp fast-count *fast-count-value*

By default, the fast sending count of LLDP packets is 3.

1.12 Configuring LLDP Management Address

1.12.1 Overview

The LLDP management address is used to identify a device on the network and is transmitted in the Management Address TLV field in the basic management TLV.

The Management Address TLV is an optional basic management TLV, as shown in **Table 1-3**However, in this device, the Management Address TLV is included in the LLDPDU by default. You can use this function to configure the content to be included in the Management Address TLV. The Management Address TLV may change if you configure the LLDP packet to publish the management address. If no management address is configured, the default management address will be used in LLDP packet.

1.12.2 Restrictions and Guidelines

- In the global configuration mode or interface configuration mode, the LLDP packet management address can be configured. The management address configured in the global configuration mode has priority over that configured in the interface configuration mode. When there is a global management address, the interface management address cannot be configured.

1.12.3 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 { *ipv4-address* | *ipv6-address* }

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.

1.13 Configuring Optional TLVs that an Interface can Publish

1.13.1 Overview

You can use this function to configure types of optional TLVs that an interface can publish or not publish, so as to change the LLDPDU content in the LLDP packet sent by the interface.

- **Table 1-3**shows basic management TLVs, where Chassis ID TLV, Port ID TLV, Time To Live TLV and End Of LLDPDU TLV are mandatory and do not need to be configured. For optional TLVs (except Management Address TLV), you can use this function to configure whether to publish these optional TLVs in the LLDPDU.
- Table 1-4 shows TLVs defined by IEEE 802.1. TLV types are optional. You can use this function to configure whether to publish Port VLAN ID TLV, Port And Protocol VLAN ID TLV and VLAN Name TLV in the LLDPDU. The LLDP protocol of this product does not support sending Protocol Identity TLVs, but supports receiving TLVs of this type.
- Table 1-5 shows TLVs defined by IEEE 802.3. TLV types are optional. You can use this function to configure whether to publish these TLVs in the LLDPDU.
- Table 1-6 shows TLVs defined by LLDP-MED. TLV types are optional. You can use this function to configure whether to publish these TLVs in the LLDPDU.

1.13.2 Restrictions and Guidelines

- Run the **lldp tlv-enable basic-tlv** command to configure optional basic management TLVs that an interface can publish. Run the **no lldp tlv-enable basic-tlv** command to configure the interface not to publish optional basic management TLVs.
  - **all**: Port Description TLV, System Capabilities TLV, System Description TLV and System Name TLV in basic management TLVs.
  - **port-description**: Port Description TLV, indicating that the interface sends the interface description information of LLDPDU.
  - **system-capability**: System Capabilities TLV, which describes the main functions of the device, such as bridging, routing and relay.
  - **system-description**: System Description TLV, which describes the device hardware version, software version and operating system, etc.
  - **system-name**: System Name TLV, which describes the name of the device.
- Run the **lldp tlv-enable dot1-tlv** command to configure the interface to publish 802.1 TLV. Run the **no lldp tlv-enable dot**1**-tlv** command to configure the interface not to publish 802.1 TLVs.
  - **all**: Port VLAN ID TLV, Port And Protocol VLAN ID TLV and VLAN Name TLV in 802.1 TLVs.
  - **port-vlan-id**: Port VLAN ID TLV, indicating port VLAN identifier.
  - **protocol-vlan-id** [*vlan-id*]: Port And Protocol VLAN ID TLV, indicating port and VLAN identifiers. *vlan-id* indicates the protocol VLAN ID of the interface. The value range is 1-4094.
  - **vlan-name** [*vlan-id*]: VLAN Name TLV, indicating VLAN name of the interface. *vlan-id* indicates the protocol VLAN ID of the interface. The value range is 1-4094.
- Run the **lldp tlv-enable dot3-tlv** command to configure the interface to publish 802.3 TLVs. Run the **no lldp tlv-enable dot3-tlv** command to configure the interface not to publish 802.3 TLVs.
  - **all**: All optional TLVs in 802.3 TLVs.
  - **link-aggregation**: Link Aggregation TLV, which describes the link aggregation capability and current aggregation state of the interface.
  - **mac-physic**: MAC/PHY Configuration/Status TLV, which describes the duplex status of the interface, the support of the automatic negotiation function and the disable or enable state of the function.
  - **max-frame-size**: Maximum Frame Size TLV, which describes the maximum size of frames that can be transmitted by the interface.
  - **power**: Power Via MDI TLV, which describes the power supply capability of the interface.
- Run the **lldp tlv-enable med-tlv** command to configure the interface to publish LLDP-MED TLVs. Run the **no lldp tlv-enable med-tlv** command to configure the interface not to publish LLDP-MED TLVs.
  - **all**: The **all** parameter in the **lldp tlv-enable med-tlv** command indicates that the interface can publish all LLDP-MED TLVs except the Location Identification TLV. The **all** parameter in the **no lldp tlv-enable med-tlv** indicates that the interface does not publish all LLDP-MED TLVs, including the Location Identification TLV.
  - **capability**: LLDP-MED Capabilities TLV, which describes whether the device supports LLDP-MED, LLDP-MED TLV type encapsulated in LLDPDU, and current device type (network connecting device or client).

- **inventory**: Describes the media device directory management TLV, including hardware version, firmware version, software version, serial number, vendor name, module name, asset identifier, etc.
- **power-over-ethernet**: Extended Power-via-MDI TLV, which indicates extended power supply capacity of the interface.
- **location civic-location identifier** *id*: City location information in Location Identification TLV, including general address and device type. **identifier** *id* is the configured city location policy ID, and the value range is 1-1024. The LLDP city location information must be configured before the TLV can be published. See **Configuring Interface to Publish City Location** for details.
- **location elin identifier** *id*: Emergency contact number information in Location Identification TLV. **identifier** *id* is the configured emergency contact number policy ID, and the value range is 1-1024. LLDP emergency contact number information must be configured first before the TLV can be published. See **Configuring Interface to Publish Emergency Contact Number** for details.
- **network-policy profile** [*profile-number*]: Network Policy TLV, which advertises VLAN configuration, supported application types (such as voice or video), Layer 2/Layer 3 priority information of the interface. *profile-number* indicates the network policy ID, with a value range of 1-1024. When the device is connected to an IP phone, if the IP phone supports LLDP-MED, you can configure the Network Policy TLV to issue policies to the IP phone. You must first configure the Network Policy TLV policy, and then configure to allow the interface to publish this TLV. See **Configuring Interface to Publish Network Policy TLV** for details.

You can run the **show lldp tlv-config** [**interface** *interface-type interface-number*] command to view the TLV publish status on the interface, where the value of the STATUS field indicates the publish status. The value of the DEFAULT field indicates the default publish status.

- Follow the following steps to configure the interface to publish TLVs:
  a Allow the interface to publish LLDP 802.3 MAC/PHY Configuration/Status TLV.
  b Allow the interface to publish LLDP-MED Capabilities TLV.
  c Allow the interface to publish other types of LLDP-MED TLVs except Network Policy TLV.
- Follow the following steps to configure the interface not to publish TLVs:
  a Configure the interface not to publish other TLVs in LLDP-MED except the Network Policy TLV.
  b Configure the interface not to publish LLDP-MED Capabilities TLV.
  c Configure the interface not to publish MAC/PHY Configuration/Status TLV.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(4) Configure the interface to publish TLVs. Configure at least one of following items.

- Configure the interface to publish optional basic management TLVs except Management Address TLV.

  lldp tlv-enable basic-tlv { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }

  By default, the interface publishes Port Description TLV, System Capabilities TLV, System Description TLV, and System Name TLV.

- Configure the interface to publish 802.1 TLVs except Protocol Identity TLV.

  lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] }

  By default, the interface publishes Port VLAN ID TLV, Port And Protocol VLAN ID TLV, and VLAN Name TLV.

- Configuration the interface to publish 802.3 TLVs.

  lldp tlv-enable dot3-tlv { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

  By default, the interface publishes all 802.3 TLVs.

- Configuration the interface to publish LLDP-MED TLVs.

  lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location civic-location identifier** *id* | **location elin identifier** *id* | **network-policy profile** [*profile-number*] | **power-over-ethernet** }

  By default, the interface publishes all LLDP-MED TLVs except Location Identification TLV.

1.14 Configuring Interface to Publish City Location

1.14.1 Overview

As shown in Table 1-6, the Location Identification TLV field in LLDP-MED TLV contains city location information (common address, device type) and emergency contact number, which are used to accurately locate endpoint devices in applications such as network topology collection.

You can use this function to configure the interface to publish city location information (common address, device type). First, create an LLDP Civic Address policy, and enter the LLDP Civic Address configuration mode to configure the common address and device type. Next, enter the interface configuration mode of a specified interface, and configure the interface to publish the city location information (common address, device type) in the Location Identification TLV.

1.14.2 Restrictions and Guidelines

- Use the **lldp location civic-location identifier** *id* to create an LLDP Civil Address policy, and enter the LLDP Civil Address configuration mode.
- In the LLDP Civic Address configuration mode, use the **civic-location** command to configure the common address information of the device. This parameter has two parts: address type *ca-type* and address information *ca-word*. The **civic-location** keyword is not reflected in the configuration command. The configuration starts with the parameter of the address type *ca-type*. Use the *ca-type ca-word* command to configure the address of the device, and use the **no** *ca-type* command to delete the address information.
- Optional parameters of address type *ca-type* include: **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**; and **additional-code**.

- Use the Address information *ca-word* field to configure specific information. Note that when the address type is **country**, use only two characters to represent the country. For example, **country** CH represents China.
- In the LLDP Civic Address configuration mode, use the **device-type** *device-type* command to to configure the device type. The default value of *device-type* is 1. The value 0 indicates a DHCP Server, 1 indicates a switch, and 2 indicates an LLDP MED client. You can use the **no device-type** command to restore the default configuration.
- In the interface configuration mode, use the **lldp tlv-enable med-tlv location civic-location identifier** *id* command to configure the interface to publish LLDP city location information (common address, device type). **med-tlv** indicates that the published information is encapsulated in LLDP MED TLV (Link Layer Discovery Protocol Media Endpoint Discovery). **location civic-location identifier** *id* indicates that the interface is allowed to publish the city location information in the Location Identification TLV. The policy ID of this information is id, and the value range is 1-1024. The LLDP city location information must be configured before the TLV can be published.
- Multiple city location information policies can be configured. You can use the **lldp tlv-enable med-tlv location civic-location identifier** *id* command on different interfaces to publish different city location information TLVs.
- You can use the **show lldp location civic-location** { **identifier** *id* | **interface** *interface-type interface-number* | **static** } command to view the configuration result.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a LLDP city location information, and enter the LLDP Civil Address configuration mode.

lldp location civic-location identifier *id*

By default, no LLDP city location information exists.

(4) Configure the city location information.

a Configure common 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*

By default, no common address information exists.

b Configure the device type information.

device-type *device-type*

By default, the device type is switch.

c Exit the global configuration mode.

exit

(5) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(6) Configure the interface to publish LLDP city location information.

lldp tlv-enable med-tlv location civic-location identifier *id*

By default, the interface does not publish LLDP city location information.

1.15 Configuring Interface to Publish Emergency Contact Number

1.15.1 Overview

As shown in Table 1-6, the Location Identification TLV field in LLDP-MED TLV contains city location information (common address, device type) and emergency contact number, which are used to accurately locate endpoint devices in applications such as network topology collection.

You can use this function to configure the interface to publish emergency contact number. First, configure an LLDP emergency contact number policy, and configure the emergency contact number. Next, enter the interface configuration mode of a specified interface, and configure the interface to publish the emergency contact number in the Location Identification TLV.

1.15.2 Restrictions and Guidelines

- In the global configuration mode, use the **lldp location elin identifier** *id* **elin-location** *telephone-number* command to configure an emergency contact number policy and telephone number.
- In the interface configuration mode, use the **lldp tlv-enable med-tlv location elin identifier** *id* command to configure the interface to publish LLDP emergency contact number. **med-tlv** indicates that the emergency contact number is encapsulated in LLDP MED TLV (Link Layer Discovery Protocol Media Endpoint Discovery). **location elin identifier** *id* indicates that the interface is allowed to publish the emergency contact number in the Location Identification TLV. The value range of the policy ID is 1-1024. LLDP emergency contact number must be configured first before the TLV can be published.
- Multiple emergency contact numbers can be configured. You can use the **lldp tlv-enable med-tlv location elin identifier** *id* command on different interfaces to allow the interface to publish different emergency contact number TLVs.
- You can use the **show lldp location elin-location** { **identifier** *id* | **interface** *interface-type interface-number* | **static** } command to view the configuration result.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the emergency contact number of the device.

lldp location elin identifier *id* **elin-location** *telephone-number*

By default, no emergency contact number exists.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(5) Configure the interface to publish LLDP emergency contact number.

lldp tlv-enable med-tlv location elin identifier *id*

By default, the interface does not publish LLDP emergency phone number.

1.16 Configuring Interface to Publish Network Policy TLV

1.16.1 Overview

If the downstream IP phone supports LLDP (Link Layer Discovery Protocol), when it goes online, it will actively send LLDP packets. If the device is configured with LLDP Network Policy TLV, it can capture LLDP packets sent by the IP phone and send Voice VLAN policies to the IP phone. If a policy is configured to allow the IP phone to send tagged frames, and the IP phone supports sending tagged packets, the IP phone will add VLAN tags when sending voice packets according to the policy. If the policy requires the IP phone to send an untagged frame, the IP phone will send untagged packets.

1.16.2 Restrictions and Guidelines

- **network-policy profile** [*profile-number*]: Allow the interface to publish Network Policy TLV and advertise the VLAN configuration of the interface, supported application types (such as voice or video), Layer 2/Layer 3 priority information, etc. *profile-number* indicates the network policy ID, with a value range of 1-1024. When the device is connected to an IP phone, if the IP phone supports LLDP-MED, you can configure the Network Policy TLV to issue policies to the IP phone. You must first configure the Network Policy TLV policy, and then configure the interface to publish this TLV.
- **voice**: Specifies the application type of Voice. **voice-signaling**: Specifies the application type of voice signaling. One LLDP Network Policy can only have one Voice application type and one Voice Signaling application type. Voice and Voice Signaling application types can exist at the same time.
- { *vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]: Configures to send tagged frames in Voice VLAN.
  - *vlan-id*: Voice VLAN ID of the voice stream in the VLAN Tag. The value range is 1-4094. The voice packet will be tagged with this ID.
  - **dot1p**: VLAN ID as 0 in the VLAN Tag, that is, the frame contains only the priority information *cos* and *dscp*.
  - **cos** *cos*: CoS (Class of Service) value of Voice VLAN voice traffic priority in the VLAN Tag. The value range is 0-7, and the default value is 5. The higher the value, the higher the priority. Ordinary VLAN packets has a CoS value of 0, with the lowest priority. By default, the CoS value of voice traffic packets entering Voice VLAN is increased to 6, which is higher than the priority of ordinary VLAN packets. The

CoS value represents the Layer 2 priority, which is stored in the Layer 2 header of the packet and filled in the PRI field of the 802.1Q VLAN Tag.

- **dscp** *dscp*: DSCP (Differentiated Services Code Point) value of Voice VLAN voice traffic priority. The value range is 0-63, and the default value is 46. The higher the value, the higher the priority. The DSCP value of ordinary IP packets is 0, with the lowest priority. The default value of Voice VLAN voice traffic packets has a DSCP value of 46, which is higher than that of ordinary IP packets. The DSCP value represents the IP priority (IP PRE) and is stored in the Layer 3 header of the packet. For IPv4 packets, the DSCP value is filled in the first six bits (bit0-bit5) of the ToS domain of the IPv4 packet header.

  For IPv6 packets, the DSCP value is filled in the first 6 bits of Traffic Class field of the IPv6 packet header.

- **untagged**: Configures the VoIP device to send untagged frames. No VLAN ID or CoS values exist in the frame. The DSCP value exists in the IP header and cannot be configured using this command.
- **none**: Indicates that the LLDP network policy is not issued (that is, the default case), and the VoIP device determines the frame to be sent according to its own configuration.

In addition to creating LLDP Network Policy on the device, you also need to:

- Enable the Voice VLAN function, and statically add the interface connecting the IP phone to the Voice VLAN. If the downstream IP phone does not support LLDP-MED, you need to manually configure the MAC address of the IP phone to the Voice VLAN OUI list. See *Configuring Voice VLA*N for details.
- Configure QoS trusted interface priority modification. See *Configuring QoS* in the *ACL and QoS Configuration Guide* for details.
- Configure a secure channel if 802.1x Authentication is also enabled on the interface, in order to allow packets in Voice VLAN to pass through. See *Configuring ACL* in the *ACL and QoS Configuration Guide* for details.
- You can use the **show lldp tlv-config** [**interface** *interface-type interface-number*] command to view the TLV publish status on the interface. The STATUS field indicates the configured publish status, and the DEFAULT field indicates the default publish status.

1.16.3 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 LLDP Network Policy configuration mode.

lldp network-policy profile *profile-number*

By default, no LLDP network policy exists.

(4) Configure the Voice VLAN policy. The following configuration tasks are exclusive. Configure one of the following items.

- Configure the Voice VLAN policy to instruct IP phone to send tagged frames.

  { **voice** | **voice-signaling** } **vlan** { *voice-vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*]

  By default, no Voice VLAN policy exists.

- Configure the Voice VLAN policy to instruct the IP phone to send untagged frames. In this case, the interface can only be manually added to the Voice VLAN.

  { **voice** | **voice-signaling** } **vlan untagged**

  By default, no Voice VLAN policy exists.

- Cancel the Voice VLAN policy, and the IP phone determines the frame to be sent according to its own configuration.

  { **voice** | **voice-signaling** } **vlan none**

  By default, no Voice VLAN policy exists.

(5) Exit the global configuration mode.

exit

(6) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(7) Configure the interface to publish the Network Policy TLV policy.

lldp tlv-enable med-tlv network-policy profile *profile-number*

By default, the interface publishes the Network Policy TLV.

1.17 Configuring the Device to Ignore PVID Detection

1.17.1 Overview

You can configure the device to ignore PVID detection on the device.

1.17.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the device to ignore PVID detection.

lldp ignore pvid-error-detect

The device does not ignore PVID detection by default,

1.18 Configuring Compatibility with Competitor Device Discovery

1.18.1 Overview

You can configure the compatibility with competitive device discovery function on the device.

1.18.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the compatibility with competitive device discovery function.

lldp compliance vendor

By default, the compatibility with competitive device discovery function is disabled.

1.19 Configuring LLDP Alarm Function

1.19.1 Overview

LLDP alarm function, namely LLDP Trap. By configuring the LLDP alarm function, you can send the LLDP information of the local device (such as discovering a new neighbor, detecting a communication link failure with a neighbor, and so on) to the network management server. The administrator can monitor the network operation according to this information.

To prevent the LLDP alarm information from being sent too frequently, the interval for sending LLDP alarms can be configured in the global configuration mode. During this interval, if LLDP information changes are detected, an alarm will be sent to the network management server.

1.19.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the interval for sending LLDP alarms.

lldp timer notification-interval *trap*

By default, the interval for sending LLDP alarm is 5 seconds.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(5) Enable the LLDP alarm function.

lldp notification remote-change enable

By default, the LLDP alarm function is disabled.

1.20 Configuring LLDP Error Detection Function

1.20.1 Overview

After this function is enabled, when an error is detected by the LLDP, a system log will be printed out and sent to the administrator.

Errors to be detected include VLAN configuration detection, interface status detection, interface aggregation configuration detection, MTU configuration detection and loop detection at both ends of the link.

1.20.2 Restrictions and Guidelines

- The LLDP error detection function depends on the devices at both ends of the link to send and receive specific TLVs in the LLDP packet. For this function to work properly, correct TLVs must be published by the device.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

- Enter the Layer 3 Ethernet interface configuration mode.

  interface { *ethernet-type interface-number* | **range** *ethernet-type interface-range* }

(4) Enable the LLDP error detection function.

lldp error-detect

By default, the LLDP error detection function is enabled.

1.21 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 contact number of the local device.
show lldp neighbors [interface *interface-type interface-number*] [**detail** | **enhance**]	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.
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.

1.22 Configuration Examples

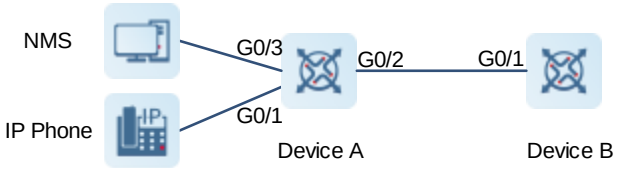
1.22.1 Checking the Neighbors Connected to the Device by Using the LLDP Function

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 Topology of Checking the Neighbors Connected to the Device by Using the LLDP Function



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
```

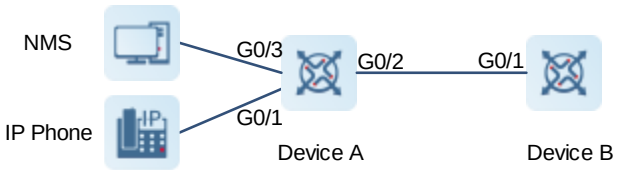
1.22.2 Configuring the LLDP Error Detection Function

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 interface, and port MTU, an error will be prompted if the configurations do not match those on the connected neighbor.

2. Topology

Figure 1-5 Topology of the LLDP Error Detection Function



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. Configuring ARP
2. Configuring IPv4 Basics
3. Configuring DHCP
4. Configuring DHCP Client
5. Configuring DHCP Snooping
6. Configuring DNS
7. Configuring IPv6 Basics
8. Configuring DHCPv6
9. Configuring DHCPv6 Client
10. Configuring DHCPv6 Snooping
11. Configuring ND Snooping
12. Configuring TCP
13. Configuring IP REF

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 Configuring Dynamic ARP Learning 9
1.4.6 Configuring Strict Dynamic ARP Learning 9
1.4.7 Configuring ARP Scanning 10
1.4.8 Configuring Scheduled Automatic ARP Scanning 10
1.5 Configuring ARP Entry Management 11
1.5.1 Overview 11

1.5.2 Configuration Tasks 11
1.5.3 Configuring a Limit on the Number of Unresolved ARP Entries 12
1.5.4 Configuring an ARP Learning Limit for an Interface 12
1.5.5 Configuring Fast ARP Entry Aging for an Interface 13
1.5.6 Configuring ARP Packet Rate Statistics Collection 13
1.5.7 Configuring the ARP Alarm Rate Limit 14
1.6 Enabling Trusted ARP 14
1.6.1 Overview 14
1.6.2 Procedure 15
1.7 Enabling Gratuitous ARP 15
1.7.1 Overview 15
1.7.2 Restrictions and Guidelines 15
1.7.3 Procedure 15
1.8 Enabling Proxy ARP 16
1.8.1 Overview 16
1.8.2 Procedure 16
1.9 Configuring Local Proxy ARP 17
1.9.1 Overview 17
1.9.2 Restrictions and Guidelines 17
1.9.3 Procedure 17
1.10 Configuring Any IP ARP 17
1.10.1 Overview 17
1.10.2 Restrictions and Guidelines 17
1.10.3 Procedure 18

1.11 Enabling ARP Trust Detection 18
1.11.1 Overview 18
1.11.2 Restrictions and Guidelines 19
1.11.3 Procedure 19
1.12 Enabling ARP-based IP Guard 19
1.12.1 Overview 19
1.12.2 Procedure 20
1.13 Configuring ARP Packet Filtering 20
1.13.1 Overview 20
1.13.2 Procedure 20
1.14 Restraining the Device from Sending ARP Requests to Authenticated VLANs 21
1.14.1 Overview 21
1.14.2 Restrictions and Guidelines 21
1.14.3 Procedure 21
1.15 Configuring Host Existence Judgment Prior to Proxy ARP Service 21
1.15.1 Overview 21
1.15.2 Restrictions and Guidelines 22
1.15.3 Procedure 22
1.16 Configuring ARP Entry Update During Active/Standby Switchover 22
1.16.1 Overview 22
1.16.2 Procedure 22
1.17 Sending ARP Requests to a Specific Sub VLAN 23
1.17.1 Overview 23
1.17.2 Procedure 23

1.18 Configuring ARP Learning for a Specific Network Segment 23
1.18.1 Overview 23
1.18.2 Procedure 23
1.19 Configuring ARP Probing Upon MAC Address Flapping 24
1.19.1 Overview 24
1.19.2 Procedure 24
1.20 Enabling Fast ARP Entry Deletion When a Layer 2 Interface Is Down 24
1.20.1 Overview 24
1.20.2 Procedure 25
1.21 Monitoring 25
1.22 Configuration Examples 26
1.22.1 Configuring Proxy ARP 26

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.

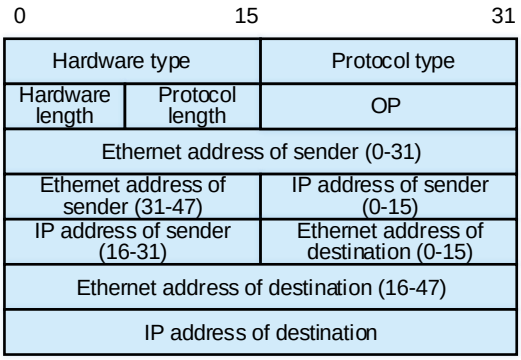
ARP maps an IP address into a MAC address. The mappings of IP and MAC addresses are stored in the ARP cache of the network device.

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



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

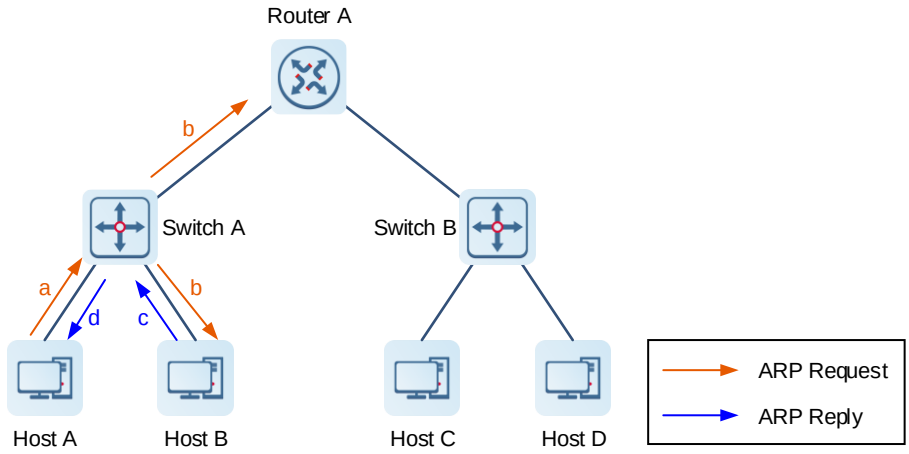
Static ARP entries are fixed mappings of IP and MAC addresses and they are created manually by the network administrator. The device cannot update the ARP entries. Static ARP entries can be deployed when communication security is a priority and network resources are sufficient.

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.

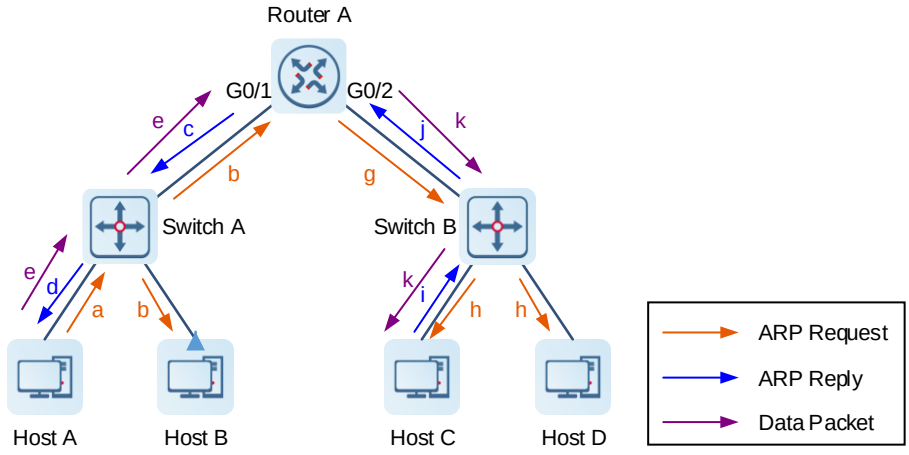
c After host B receives the ARP request, host B adds the MAC address of host A to its ARP table, and sends an ARP reply to host A. Since the destination IP address of the ARP request is not the IP address of router A, router A directly discards the ARP request after receiving it.

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 device, and adds trusted ARP entries on the user's gateway device. 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
  - Configuring ARP Learning for a Specific Network Segment
  - Enabling Fast ARP Entry Deletion When a Layer 2 Interface Is Down

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 a 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*] *ipv4-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
- Configuring 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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 for the first ARP request, the ARP request packet will be retransmitted for four consecutive times.

1.4.5 Configuring 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(4) Configure dynamic ARP learning.

- Configure dynamic ARP to learn only IPv4 addresses in the specified range.

  arp-learning *start-ipv4-address* [*end-ipv4-address*]

- 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(4) Enable ARP scanning.

arp scan [*start-ipv4-address end-ipv4-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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(4) Enable scheduled automatic ARP scanning.

arp scan auto [*start-ipv4-address end-ipv4-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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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.

- Enter the SVI configuration mode.

  interface vlan *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) Enable the function of learning gratuitous ARPs.

(4) The function of learning gratuitous ARPs is enabled by default.Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(5) Enable the function of sending gratuitous ARP requests.

arp gratuitous-send enable

The function of sending gratuitous ARP requests is enabled by default.

(6) 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 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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.

- Enter the SVI configuration mode.

  interface vlan *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(4) Enable any IP ARP.

arp any-ip [**dip-route**]

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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.

- Enter the SVI configuration mode.

interface vlan *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.

This command is supported only when the device is in VSU mode.

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 broadcast resolution requests to a specific sub VLAN in a super VLAN.

arp resolve vlan { *vlan-list* | **none** }

ARP broadcasts resolution requests to all sub VLANs in a super VLAN by default.

1.18 Configuring ARP Learning for a Specific Network Segment

1.18.1 Overview

When you manage a specific network segment of a Layer 3 interface, run the **arp disable-learning** command to disable ARP learning of the specific network segment. After configuration, the interface does not learn any dynamic ARP of the network segment. Note that after disabling ARP learning of the specific network segment, the device does not automatically delete the existing dynamic ARP on the network segment. After the user goes offline, the device deletes aging ARPs. To delete it immediately, run the **clear arp-cache ipv4-address mask** command to clear the dynamic ARPs on the network segment.

1.18.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *interface-number*

(4) Disable dynamic ARP learning of a specific network segment.

arp disable-learning *network-address mask*

The function is not configured on an interface by default.

1.19 Configuring ARP Probing Upon MAC Address Flapping

1.19.1 Overview

When MAC address flapping occurs (that is, when the Layer 2 interface in a MAC address entry changes to another one different from the Layer 2 interface in the mapping ARP entry), a device immediately updates the Layer 2 interface in the mapping ARP entry by default. To prevent a device from updating the Layer 2 interface in the mapping ARP entry to an incorrect one when attacked, you can enable ARP probing upon MAC address flapping. After the function is enabled, the device will send unicast ARP probe packets to the new interface and the old one, respectively. If an ARP response is received, the Layer 2 interface in the ARP entry will be updated to the one that sends the response. If no ARP response is received, the Layer 2 interface in the ARP entry will be updated to the new one after ARP probing.

1.19.2 Procedure

(5) Enter the privileged EXEC mode.
enable

(6) Enter the global configuration mode.
configure terminal

(7) Enable ARP probing upon MAC address flapping.
arp mac-flapping resolve enable

ARP probing upon MAC address flapping is disabled by default.

(8) Configure an interval for ARP probing upon MAC address flapping.
arp mac-flapping resolve interval *seconds*

ARP probing is performed upon MAC address flapping at an interval of two seconds by default.

(9) Configure the number of times for ARP probing upon MAC address flapping.
arp mac-flapping resolve times *number*

ARP probing is performed upon MAC address flapping five times by default.

1.20 Enabling Fast ARP Entry Deletion When a Layer 2 Interface Is Down

1.20.1 Overview

ARP entries are deleted when the aging time expires by default. To accelerate routing convergence, enable fast ARP entry deletion when a Layer 2 interface is Down. When this function is enabled on an SVI and a Layer 2 interface of the SVI goes Down, the device deletes ARP entries immediately.

1.20.2 Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Enter the SVI configuration mode.
interface vlan *interface-number*

(4) Enable fast ARP entry deletion when a Layer 2 interface is Down.
arp l2port-down fast-delete

ARP entries are not deleted immediately when a Layer 2 interface is Down by default.

1.21 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 [*ipv4-address* [*mask*]]	Displays trusted ARP entries.
clear arp-cache [**vrf** *vrf-name*] **trusted** [*ipv4-address* [*mask*]]	Clears trusted ARP entries.
clear arp-cache [[**vrf** *vrf-name*] [*ipv4-address* [*mask*] | **vxlan**] | **interface** *interface-type interface-number*]	Clears dynamic ARP entries.
clear arp-cache packet statistics [*interface-type interface-number*]	Clears ARP packet statistics.

show arp [*interface-type interface-number* | **trusted** [*ipv4-address* [*mask*]] | [**vrf** *vrf-name*] [*ipv4-address* [*mask*] | *mac-address* | **complete** | **incomplete** | **static**]]	Displays the ARP table.
show arp detail [*interface-type interface-number* | [**trusted** [*ipv4-address* [*mask*]]] | [**vrf** *vrf-name*] [*ipv4-address* [*mask*] | *mac-address* | **complete** | **incomplete** | **static**] | **subvlan** { **min-max** *min-value max-value* | *subvlan-number* }]	Displays the detailed ARP table.
show ip arp [**vrf** *vrf-name*]	Displays the ARP table.
show arp [**detail**] **trusted** [*ipv4-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** *interface-type interface-number*]	Displays ARP packet rate statistics.
show arp flapping record [*ipv4-address*]	Displays ARP flapping records.
show arp anti-attack statistics	Displays the statistics on illegal ARP packets.
debug arp	Displays the statistics on ARP packets sent and received.
debug arp event	Displays the creation and deletion status of ARP entries.

1.22 Configuration Examples

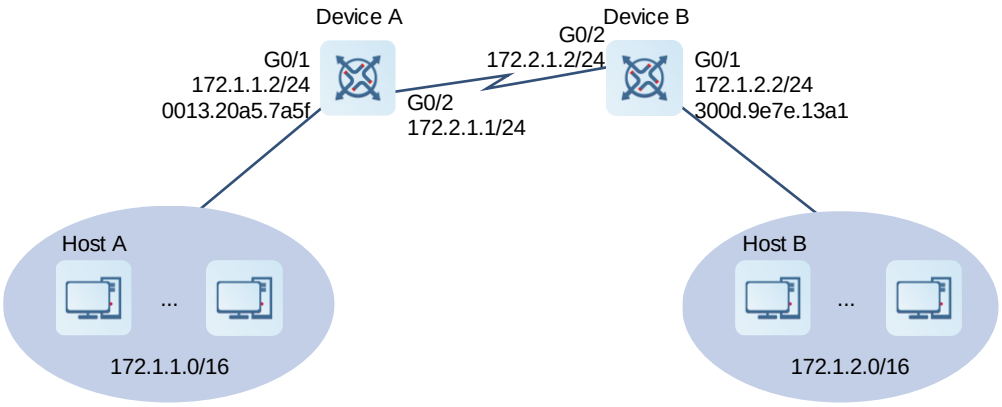
1.22.1 Configuring Proxy ARP

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 a Layer 3 Ethernet 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 a Layer 3 Ethernet 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 a Layer 3 Ethernet 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 a Layer 3 Ethernet 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 a Layer 3 Ethernet 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 a Layer 3 Ethernet 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 172.1.1.1/24.

Set the IP address of host B to 172.1.2.1/24.

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 a Layer 3 Ethernet port GigabitEthernet 0/1 on device A.

6. Configuration Files

- Device A configuration file

```
!
hostname DeviceA
ip route 172.1.0.0 255.255.0.0 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 172.1.0.0 255.255.0.0 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 7
1.3.1 Overview 7
1.3.2 Configuration Tasks 7
1.3.3 Configuring a Static IP Address for an Interface 8
1.3.4 Configuring an IP Address Combination for an Interface 8
1.3.5 Configuring an IP Broadcast Address 9
1.4 Configuring Directed Broadcast Packets 9
1.4.1 Overview 9
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure 10
1.5 Configuring ICMP Messages 10
1.5.1 Overview 10
1.5.2 Configuration Tasks 10
1.5.3 Enabling the Function of Sending TTL Timeout Messages 10
1.5.4 Enabling the Timestamp Query 11

1.5.5 Enabling the Function of Sending ICMP Destination Unreachable Messages 11
1.5.6 Enabling the Function of Sending ICMP Redirection Messages 11
1.5.7 Enabling the Function of Sending ICMP Mask Reply Messages 12
1.6 Configuring the Transmission Rate of ICMP Error Messages 12
1.6.1 Overview 12
1.6.2 Restrictions and Guidelines 12
1.6.3 Procedure 12
1.7 Setting the IP MTU Value 13
1.7.1 Overview 13
1.7.2 Restrictions and Guidelines 13
1.7.3 Procedure 13
1.8 Configuring the IP Fragment Reassembly 13
1.8.1 Overview 13
1.8.2 Procedure 14
1.9 Setting the IP TTL Value 14
1.9.1 Overview 14
1.9.2 Procedure 14
1.10 Configuring the IP Source Route Option 14
1.10.1 Overview 14
1.10.2 Restrictions and Guidelines 14
1.10.3 Procedure 14
1.11 Monitoring 15
1.12 Configuration Examples 15
1.12.1 Configuring IPv4 Addresses for Network Communication 15

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

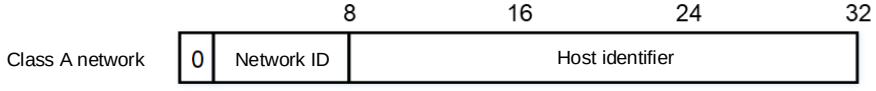
1. Classification of IP Addresses

IP addresses are used for interconnection at the IP layer. An IP address consists of 32-bit binary digits. 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.

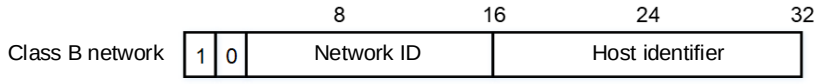
- For a class A address, the most significant bit is "0", the following 7 bits indicate a network ID, and the last 24 bits indicate a local address (host identifier). There are 2^7 = 128 class A networks in total.

Figure 1-1 Class A Network



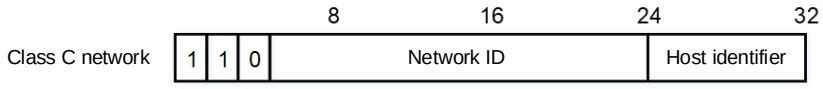
- For a class B address, the two most significant bits are "10", the following 14 bits indicate a network ID (network identifier), and the last 16 bits indicate a local address (host identifier). There are 2^{14}=16,384 class B networks in total.

Figure 1-2 Class B Network



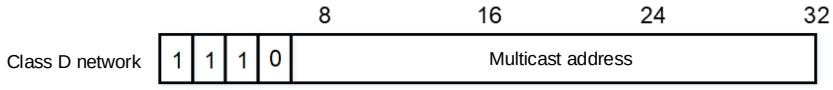
- For a class C address, the three most significant bits are "110", and the following 21 bits indicate a network ID, and the last 8 bits indicate a local address. There are 2^{21}=2,097,152 class C networks in total.

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 RFC 1918 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 RFC 1166.

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, in bytes, of the data transmitted by the data link layer to its upper layer, such as IP. 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. When two hosts communicate through multiple networks, MTUs of different sizes may exist in every link. 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.

When two hosts communicate through multiple networks, 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 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 multiple 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 RFC 919 and RFC 922.

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

  RFC 792 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 other 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 RFC 791. 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

- RFC 1918: Address Allocation for Private Internet
- RFC 1166: Internet Numbers
- RFC 919: Broadcasting Internet Datagrams
- RFC 922: Broadcasting Internet Datagrams Subnets
- RFC 791: Internet Protocol
- RFC 792: 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 Directed Broadcast Packets
- Configuring ICMP Messages
- Configuring the Transmission Rate of ICMP Error Messages
- Setting the IP MTU Value
- Configuring the IP Fragment Reassembly
- Setting the IP TTL Value
- 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 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure an IP address for an interface.

ip address *ipv4-address* { *mask* | *mask-length* } [**secondary**]

No IP address is configured for an interface by default.

1.3.4 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.

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *interface-number*

(4) Configure an IP address combination for the interface.

ip address mix { *ipv4-address* { *mask* | *mask-length* } | **dhcp** }

No IP address combination is configured for an interface by default.

1.3.5 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Configure an IP broadcast address.

ip broadcast-address *ipv4-address*

The default IP broadcast address of an interface is 255.255.255.255.

1.4 Configuring Directed Broadcast Packets

1.4.1 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.

1.4.2 Restrictions and Guidelines

- This function 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.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *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.

1.5 Configuring ICMP Messages

1.5.1 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.

1.5.2 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

1.5.3 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.

1.5.4 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 disabled by default.

1.5.5 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *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.

1.5.6 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Enable the function of sending ICMP redirection messages.

ip redirects

The function of sending ICMP redirection messages is enabled by default.

1.5.7 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Enable the function of sending ICMP mask reply messages.

ip mask-reply

The function of sending ICMP mask reply messages is disabled by default.

1.6 Configuring the Transmission Rate of ICMP Error Messages

1.6.1 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.

1.6.2 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.

1.6.3 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.

1.7 Setting the IP MTU Value

1.7.1 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.

1.7.2 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.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode。

  interface vlan *interface-number*

(4) Set the IP MTU.

ip mtu *mtu*

The default MTU of an IP packet is 1500 bytes.

1.8 Configuring the IP Fragment Reassembly

1.8.1 Overview

By default, a device reassembles IP packets sent to the CPU, and then determines whether to forward them or process them locally. If you do not want to reassemble the IP packets sent to the CPU, you can disable the IP fragment reassembly.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable the IP fragment reassembly function.

ip reassemble disable

The IP fragment reassembly function is enabled by default.

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 the IP Source Route Option

1.10.1 Overview

The IP source route option is used to test the throughput of a specific network and help the packet bypass a failed network.

1.10.2 Restrictions and Guidelines

Enabling the IP source route option may cause network attacks such as source address spoofing and IP spoofing.

1.10.3 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.

1.11 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 [*interface-type interface-number* | **total**]	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.

1.12 Configuration Examples

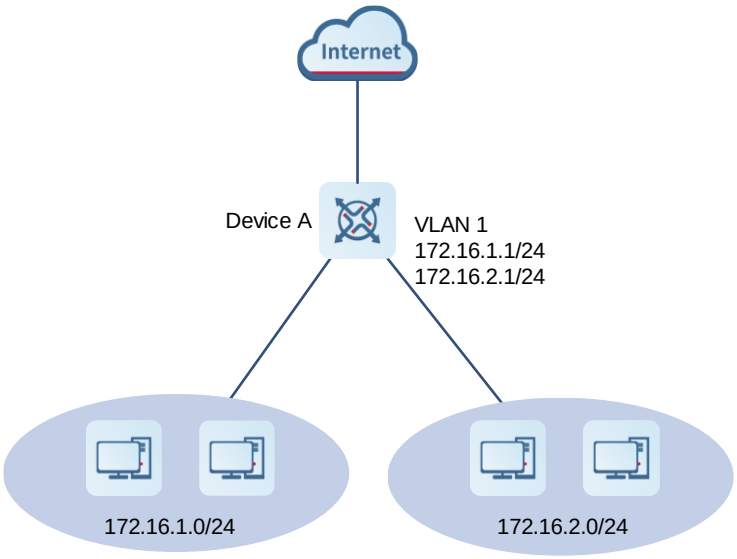
1.12.1 Configuring IPv4 Addresses for Network Communication

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 secondary 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 172.16.2.2
Sending 5, 100-byte ICMP Echoes to 172.16.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 38/45/55 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 10
1.2.7 Protocols and Standards 11
1.3 Configuring DHCP Server 11
1.3.1 Overview 11
1.3.2 Configuration Task Summary 11
1.3.3 Enabling DHCP Server 12
1.3.4 Configuring Static IP Address Assignment 12
1.3.5 Configuring Dynamic Assignment of IP Addresses and Network Parameters 13
1.3.6 Configuring DHCP Address Pool Management Function 14
1.3.7 Providing the Boot Image File Name 15
1.3.8 Assigning IP Addresses Based on Class Rules 16
1.3.9 Assigning IP Addresses Based on AM Rules 17
1.3.10 Refreshing Trusted ARP Entries 18
1.3.11 Configuring Rogue DHCP Server Detection 19

1.3.12 Configuring IP Address Exclusion.....19
1.3.13 Configuring IP Address Conflict Detection.....20
1.3.14 Configuring Compulsory NAK Reply 21
1.3.15 Configuring Preferential Assignment of External DNS Server Addresses 21
1.3.16 Configuring VRRP Monitoring.....22
1.3.17 Configuring ARP-based Go-Offline Detection 22
1.3.18 Saving Historical Leases 23
1.4 Configuring DHCP Relay.....23
1.4.1 Overview 23
1.4.2 Configuration Task Summary.....23
1.4.3 Configuring Basic DHCP Relay Functions 23
1.4.4 Configuring Option 82.....24
1.4.5 Configuring Server-ID Check.....26
1.4.6 Enabling DHCP Relay Suppression 26
1.4.7 Configuring Multiple Gateway IP Addresses 27
1.4.8 Forcing a DHCP Relay to Send a Reply Packet 27
1.4.9 Configuring the Source IP Address of DHCP Relay Packets.....28
1.5 Monitoring 28
1.6 Configuration Examples.....30
1.6.1 Configuring Static Address Binding 30
1.6.2 Dynamically Assigning IP Addresses.....32
1.6.3 Configuring DHCP Relay 34
1.6.4 Assigning IP Addresses Based on Class Rules 37

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 on the same network segment, 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. As an enhancement version of BOOTP, 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 static address assignment mode considers the real locations of hosts and the labor cost is high. A DHCP application mode only needs to be uniformly configured on a server, thereby reducing a network access cost.
- 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 agent

  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.

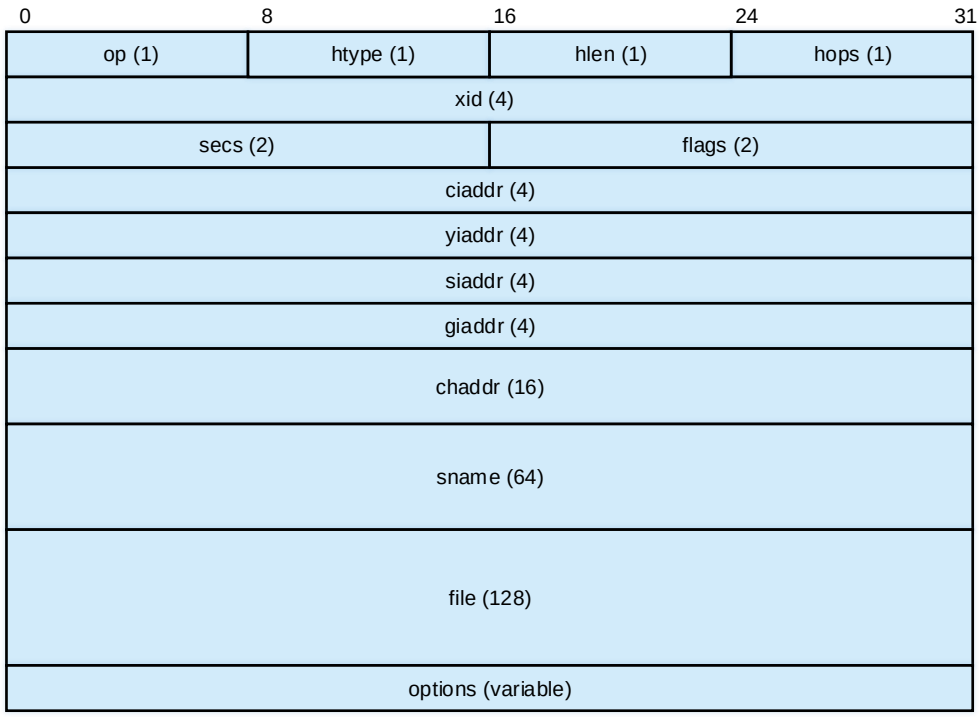
- Option type

  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, 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.

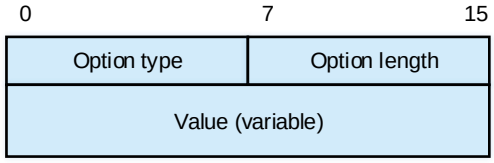
2. Message Types

- 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 DHCP server in response to a DHCP client's DHCP REQUEST message. A client obtains an IP address and related configuration parameters only after receiving this message.
- DHCP NAK: After a DHCP server receives a DHCP REQUEST message, the server cannot find the lease record or assign an IP address to the client due to some reasons. The server sends a DHCP NAK packet to inform the DHCP client that no proper IP address can be assigned.
- DHCP DECLINE: After a DHCP client receives an ACK message, the client finds that the IP address assigned by a server has been used through address conflict detection. Or the assigned IP address is unavailable due to other reasons. The client sends a DHCP DECLINE packet to inform the DHCP server that the assigned IP address is unavailable and request for a new IP address.
- DHCP REALEASE: When a DHCP client no longer uses the assigned IP address, it sends a DHCP RELEASE packet to inform the DHCP server of the assigned IP address not be used any longer and request the DHCP server to release the assigned IP address.

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.

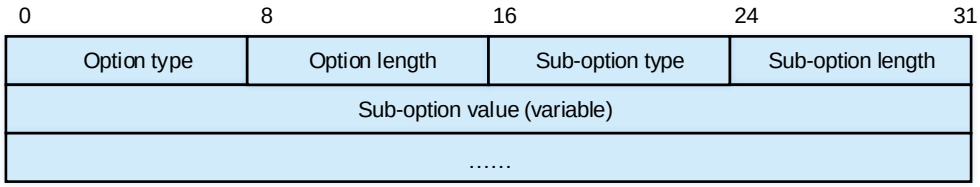
5. User-Defined DHCP Options

- 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

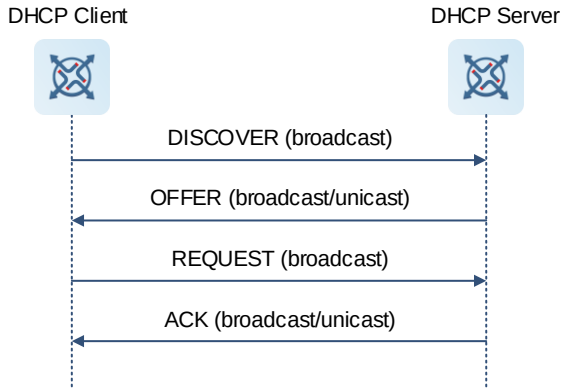


- Option 82: relay agent information

  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 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.

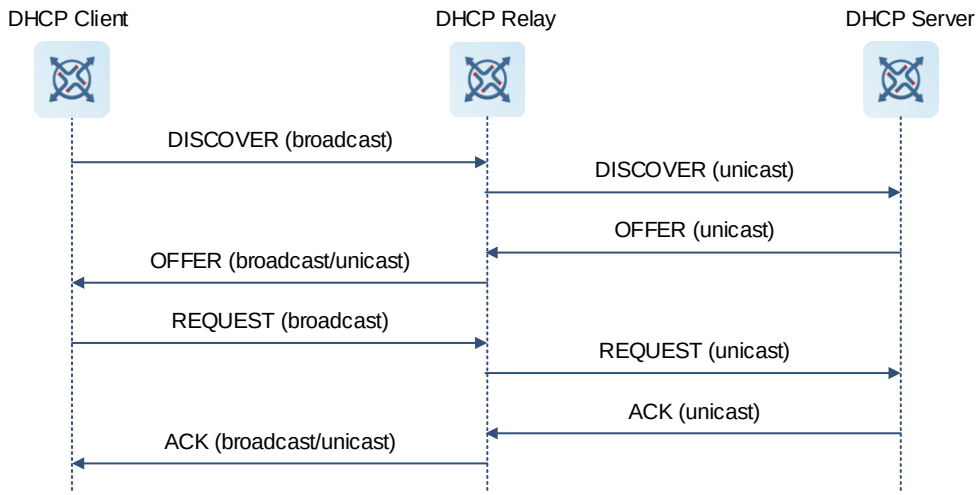
However, the DHCP server can send NAK packets only to its managed DHCP clients because it has lease records of its managed clients only. When a DHCP client moves from another network to the local network, if the DHCP server cannot find the corresponding lease record locally, the DHCP server does not 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

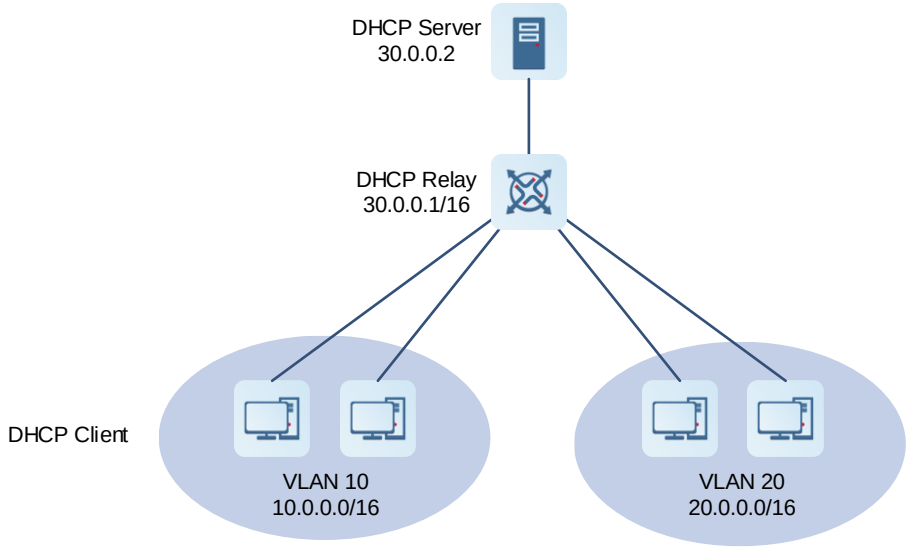


(1) After a DHCP relay agent receives a DHCP DISCOVER or DHCP REQUEST packet broadcast by a DHCP client, the DHCP relay agent adds its own IP address to the **giaddr** field of the packet and forwards the packet to a specified DHCP server in unicast mode.

(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

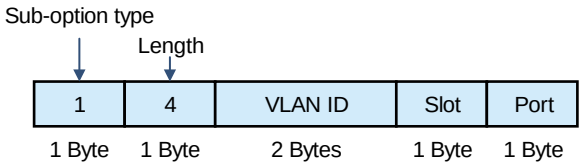
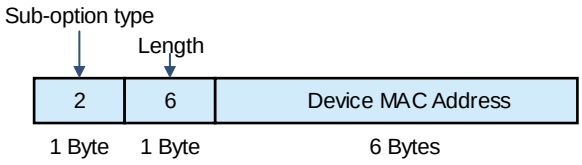


Figure 1-8 Option 82 Remote ID



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

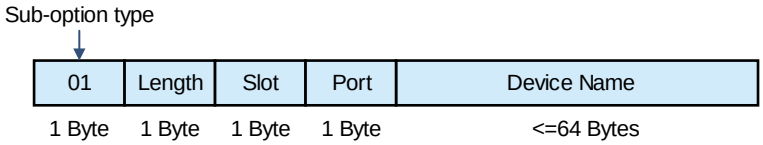
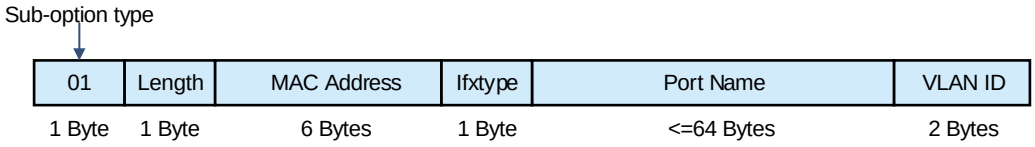


Figure 1-10 Custom Option 82 Remote ID

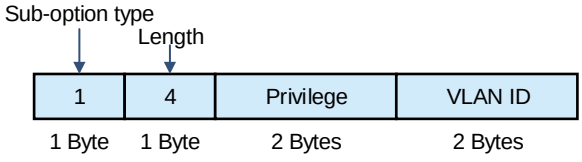


5. Option Dot1x

Option Dot1x should be used in combination with 802.1X authentication and 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



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.

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) Configuring DHCP Address Pool Management Function

(6) (Optional) Providing the Boot Image File Name

(7) (Optional) Assigning IP Addresses Based on Class Rules

(8) (Optional) Assigning IP Addresses Based on AM Rules

(9) 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

(10) Configuring other custom functions of the DHCP server: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring IP Address Exclusion
- Configuring IP Address Conflict Detection
- Configuring Compulsory NAK Reply
- Configuring Preferential Assignment of External DNS Server Addresses
- 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

Static IP address assignment is used to assign specific IP addresses and other configuration information to certain DHCP clients (such as servers and printers). This function allows you to configure multiple static IP address bindings in an address pool, greatly increasing the number of static IP address bindings. Each address pool can be configured with a maximum of 2,000 static IP address bindings. Each IP address can be bound to only one static user using either a MAC address or a client ID.

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 binding of static user addresses.

static-bind ip-address *ipv4-address* { *mask-address* | *mask-length* } { **hardware-address** *hardware-address* | **client-identifier** *unique-identifier* }

Static user address binding is not configured by default.

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 mask* [*low-ipv4-address high-ipv4-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 *ipv4-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 *ipv4-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 { *ipv4-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** *ipv4-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.

For address pools other than static address pools, you are not advised to set the lease time to permanent.

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 { **disable** | **enable** }

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) Configure the list of boot servers that a DHCP client needs to access during boot.

next-server { *ipv4-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-ipv4-address high-ipv4-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

Address management (AM) rules can be used to efficiently assign IP addresses to DHCP clients in different scenarios. In super VLAN scenarios, the AM rules can be used to plan the IP range for DHCP clients from different VLANs or ports. After an AM rule is configured, all DHCP clients from the specified VLANs ports and VNIs can obtain IP addresses. If a DHCP client is from a VLAN, port, or VNI 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. 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 *ipv4-address* { *mask* | *mask-length* }

- Configure dynamic address assignment based on the VLAN and port.

  match ip *ipv4-address* { *mask* | *mask-length* } [*interface-type interface-number*] [**add | remove**] **vlan** *vlan-id*

- Configure dynamic address assignment based on the VLAN.

  match ip *ipv4-address* { *mask* | *mask-length* } [**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.

(6) (Optional) Clear the matching rules in AM rules.

clear match ip [interface-type interface-number | **loose**]

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.

2. Restrictions and Guidelines

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.

3. 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

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure rogue server detection.

ip dhcp server detect

Rogue server detection is disabled by default.

1.3.12 Configuring IP Address Exclusion

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.

2. 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-ipv4-address* [*high-ipv4-address*]

By default, a DHCP server assigns all addresses from an IP address pool to DHCP clients.

1.3.13 Configuring IP Address Conflict Detection

1. Overview

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 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 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.

4. 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.

5. 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.

1.3.14 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.

1.3.15 Configuring Preferential Assignment of External DNS Server Addresses

1. Overview

When a device works in the Point-to-Point Protocol over Ethernet (PPPoE) or DHCP client mode, it can obtain DNS server addresses automatically from an external DHCP server. Configure the DNS server addresses on the DHCP server of the local device, so that users do not need to perform DNS configuration. When a device serves as a DHCP server, it preferentially assigns clients with a DNS server address obtained from an external DHCP server.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure preferential assignment of external DNS server addresses to clients when the device works in the DHCP client or PPPoE mode.

ip dhcp dns dynamic

By default, run the **dns-server** command to assign DNS server addresses to clients.

1.3.16 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 interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

interface vlan *interface-number*

(4) Enable VRRP monitoring.

ip dhcp monitor-vrrp-state

VRRP monitoring is disabled for an interface by default.

1.3.17 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.

1.3.18 Saving Historical Leases

1. Overview

Enable a DHCP server to save historical leases, the DHCP server saves the IP address lease of a client to the database after an IP address is assigned to a client and the client goes offline. 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 on a device. 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.

- The **service dhcp** command is used to enable both the DHCP server and DHCP relay functions. However, a device cannot function as a DHCP server and relay at the same time. When a device is configured with a valid address pool, it acts as a server. Otherwise, it serves as a relay.

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*] *ipv4-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. Restrictions and Guidelines

- Configure basic DHCP Relay functions.

3. 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.

(6) Set the **Circuit ID** sub-option in DHCP Option 82 to a user-defined hexadecimal or ASCII string.

ip dhcp relay information circuit-id format { **hex | ascii** } *string*

The **Circuit ID** sub-option in DHCP Option 82 is not set to a user-defined hexadecimal or ASCII string by default.

(7) (Optional) Set the **Circuit ID** sub-option in DHCP Option 82 to a user-defined device name.

ip dhcp relay information circuit-id string *devicename*

The **Circuit ID** sub-option in DHCP Option 82 is not set to a user-defined device name by default.

(8) (Optional) Set the **Remote ID** sub-option in DHCP Option 82 to a user-defined hexadecimal or ASCII string globally.

ip dhcp relay information remote-id format { **hex | ascii** } *string*

The **Remote ID** sub-option in DHCP Option 82 is not set to a user-defined hexadecimal or ASCII string by default.

(9) (Optional) Set the **Remote ID** sub-option in DHCP Option 82 to a user-defined interface name globally.

ip dhcp relay information remote-id string *portname*

The **Remote ID** sub-option in DHCP Option 82 is not set to a user-defined interface name by default.

(10) (Optional) Enable the function of filling DHCP Option 82 with content in Verbose format.

ip dhcp relay information verbose-opt82

The function of filling DHCP Option 82 with content in Verbose format is disabled by default.

(11) Enter interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

(12) (Optional) Set the **Remote ID** sub-option in DHCP Option 82 to a user-defined hexadecimal or ASCII string for the interface.

ip dhcp relay information remote-id format { **hex | ascii** } *string*

The **Remote ID** sub-option in DHCP Option 82 is not set to a user-defined hexadecimal or ASCII string by default.

(13) (Optional) Set the **Remote ID** sub-option in DHCP Option 82 to a user-defined interface name for the interface.

ip dhcp relay information remote-id string *portname*

The **Remote ID** sub-option in DHCP Option 82 is not set to a user-defined interface name by default.

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. Restrictions and Guidelines

3. Configure basic DHCP Relay functions. 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

By default, a DHCP relay agent forwards a DHCP Request message to all DHCP servers.

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. Restrictions and Guidelines

Configure basic DHCP Relay functions.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

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. Restrictions and Guidelines

Configure 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 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

- Configure basic DHCP Relay functions.
- Only one source IP address can be specified for DHCP relay packets on each interface.
- This function must 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *interface-number*

(4) Configure the source IP address for DHCP relay packets.

ip dhcp relay source *ipv4-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 { *ipv4-address* | ***** }	Clears DHCP address binding records.
clear ip dhcp conflict { *ipv4-address* | ***** }	Clears DHCP address conflict records.
clear ip dhcp history { *mac-address* | ***** }	Clears DHCP historical lease records.
clear ip dhcp server detect { *ipv4-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 dhcpserver exclude	Displays the excluded address range of a DHCP server.
show dhcpserver manual-bind	Displays statically bound IP addresses of a DHCP server.
show dhcpserver pool	Displays configurations of the specified IP address pool on a DHCP server.
show dhcpserver support	Displays functions supported by a DHCP server.
show ip dhcp binding	Displays DHCP address bindings.
show ip dhcp conflict	Displays address conflict records of a DHCP server.
show ip dhcp database	Displays the running status of the database backup function of a DHCP server.
show ip dhcp dns dynamic	Displays DNS server addresses obtained from an external DHCP server when the device works in the PPPoE or DHCP client mode.
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 server relay-binding [**detail**]	Displays binding information about a DHCP relay agent.
show ip dhcp server relay-ifx	Displays all interface data of a DHCP relay agent.
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.
show ip dhcp server status	Displays status of a DHCP server.
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 1-12, 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 1-12 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)# no switchport
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)# static-bind ip-address 192.1.1.99 255.255.255.0
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
!
service dhcp
!
ip dhcp pool pool1
 hardware-address 0050.56b0.2f50
 host 192.1.1.99 255.255.255.0
!
interface GigabitEthernet 0/1
 no switchport
 ip address 192.1.1.1 255.255.255.0
!
```

7. Common Errors

- No address pool is configured.
- The DHCP Server service is not enabled.

1.6.2 Dynamically Assigning IP Addresses

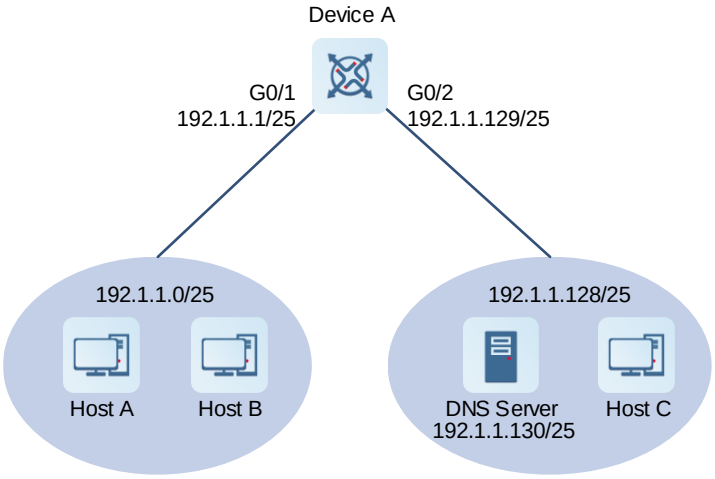
1. Requirements

As shown in Figure 1-13, 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 1-13 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)# no switchport
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)# no switchport
```

```
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    Dynamic total  Dynamic distributed  Dynamic remained  Static-bind total
Static-bind distributed     Static-bind remained  Disable/conflict  Percentage
------------  -------------  -------------------  ----------------
-----------------
----------------------     --------------------  ----------------  ----------
pool1         125           2                  123             0
0                        0                 0               0.98400
pool2         125           1                  124             0
0                        0                 0               0.80000
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
```

```
 interface gigabitethernet 0/1
 no switchport
 ip address 192.1.1.1 255.255.255.128
!
 interface gigabitethernet 0/2
 no switchport
 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.

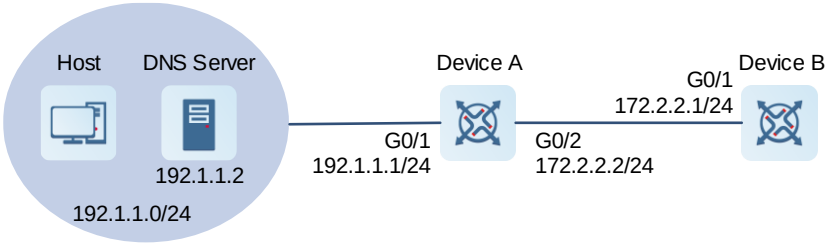
1.6.3 Configuring DHCP Relay

1. Requirements

As shown in Figure 1-14, 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 1-14 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)# no switchport
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)# no switchport
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)# no switchport
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 0/1 172.2.2.2
```

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    Dynamic total  Dynamic distributed  Dynamic remained  Static-bind total
Static-bind distributed     Static-bind remained  Disable/conflict  Percentage
------------  -------------  -------------------  ----------------
-----------------
-----------------------     --------------------  ----------------  ----------
pool1         253           1                     252               0
0                           0                     0                 0.99604
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 no switchport
 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
 no switchport
 ip address 172.2.2.1 255.255.255.0
!
 ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1 172.2.2.2
 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.

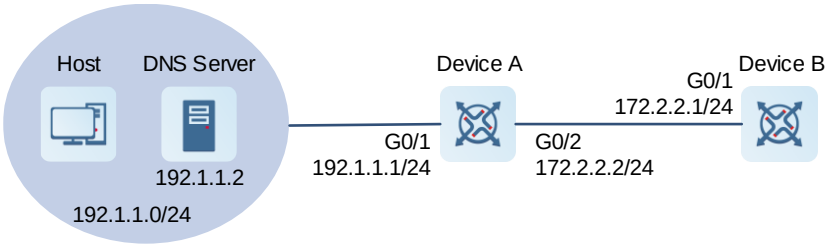
1.6.4 Assigning IP Addresses Based on Class Rules

1. Requirements

As shown in Figure 1-15, Device A serves as a DHCP relay agent to forward DHCP packets between the clients and server, and Device B serves as a DHCP server to assign IP addresses and other network configurations to the clients. 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 1-15 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)# no switchport
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)# no switchport
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)# no switchport
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 0/1 172.2.2.2
```

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 the clients that match class rules obtain IP addresses in the range of 192.1.1.200 to 192.1.1.254 and other clients obtain 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
 no switchport
 ip address 192.1.1.1 255.255.255.0
 exit
 interface gigabitethernet 0/2
 no switchport
 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 0/1 172.2.2.2
 service dhcp
!
 interface gigabitethernet 0/1
 no switchport
 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 Configuration Task Summary 2
1.3 Enabling DHCP Client Function 2
1.3.1 Overview 2
1.3.2 Restrictions and Guidelines 2
1.3.3 Procedure 2
1.4 Configuring Characteristics of DHCP Reply Packets 3
1.4.1 Overview 3
1.4.2 Configuration Procedure 3
1.5 Monitoring 3
1.6 Configuration Examples 4
1.6.1 Enabling DHCP Client Function 4

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 Configuration Task Summary

DHCP client configuration includes the following tasks:

(1) Enabling DHCP Client Function

(2) (Optional) Configuring Characteristics of DHCP Reply Packets

1.3 Enabling DHCP Client Function

1.3.1 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.

1.3.2 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.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *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.

1.4 Configuring Characteristics of DHCP Reply Packets

1.4.1 Overview

When a DHCP client requests an IP address, no detection mechanism is deployed between the client and server. Therefore, when multiple DHCP servers exist on a network, the DHCP client selects the first server that sends an Offer message to request an IP address. When multiple DHCP servers exist, DHCP clients can apply for IP addresses randomly and can be easily interfered by unauthorized DHCP servers. You can configure characteristics of DHCP Reply packets. In this case, only the server that meets the characteristics can allocate IP addresses to clients.

1.4.2 Configuration Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Entry the SVI configuration mode.
  interface vlan *interface-number*

(4) Configure characteristics of DHCP Reply packets.
ip dhcp client specify-server { **ip** *ip-address* | **option** *id* **include** { **ascii** *ascii-data* | **hex** *hex-data* | **ip** *ip-address* } }

By default, characteristics of DHCP Reply packets are not configured.

1.5 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.

1.6 Configuration Examples

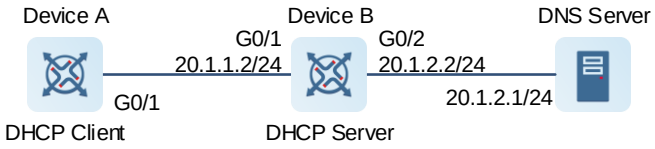
1.6.1 Enabling DHCP Client Function

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)# no switchport
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)# no switchport
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)# no switchport
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)
dev.registryg.com                     dynamic phasing
---
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 no switchport
 ip address dhcp
!
```

- Device B configuration file

```
hostname DeviceB
!
 service dhcp
 ip dhcp excluded-address 20.1.1.2
!
 interface gigabitethernet 0/1
```

```
 no switchport
 ip address 20.1.1.2 255.255.255.0
!
 interface gigabitethernet 0/2
 no switchport
 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
1.5.1 Overview 8
1.5.2 Procedure 8
1.6 Enabling Source MAC Address Verification 9
1.6.1 Overview 9
1.6.2 Procedure 9
1.7 Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time 9
1.7.1 Overview 9
1.7.2 Procedure 9
1.8 Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time 9

1.8.1 Overview 9
1.8.2 Procedure 9
1.9 Enabling DHCP Snooping to Support BOOTP Binding 10
1.9.1 Overview 10
1.9.2 Procedure 10
1.10 Enabling DHCP Snooping to Support Relay Request Packet Processing 10
1.10.1 Overview 10
1.10.2 Procedure 10
1.11 Enabling DHCP Snooping to Support Binding Entry Migration 11
1.11.1 Overview 11
1.11.2 Procedure 11
1.12 Enabling DHCP Snooping to Fast Age Client Migration Entries 11
1.12.1 Overview 11
1.12.2 Procedure 11
1.13 Enabling the Loose Forward Function for DHCP Snooping 11
1.13.1 Overview 11
1.13.2 Procedure 12
1.14 Configuring an Interface in the Suppression State 12
1.14.1 Overview 12
1.14.2 Procedure 12
1.15 Configuring the Maximum Number of Users Bound to a VLAN 12
1.15.1 Overview 12
1.15.2 Procedure 12
1.16 Configuring Option 82 13

1.16.1 Overview 13
1.16.2 Restrictions and Guidelines 13
1.16.3 Procedure 13
1.17 Enabling DHCP Snooping Monitoring 14
1.17.1 Overview 14
1.17.2 Restrictions and Guidelines 14
1.17.3 Procedure 14
1.18 Monitoring 15
1.19 Configuration Examples 15
1.19.1 Configuring DHCP Snooping 15
1.20 Common Misconfigurations 17

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 authorized 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*.

  When an interface is configured as a DHCP snooping trusted interface, the DHCP guard function of NFPP does not take effect to prevent DHCP traffic from being mistakenly blocked on the trusted interface.

- 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

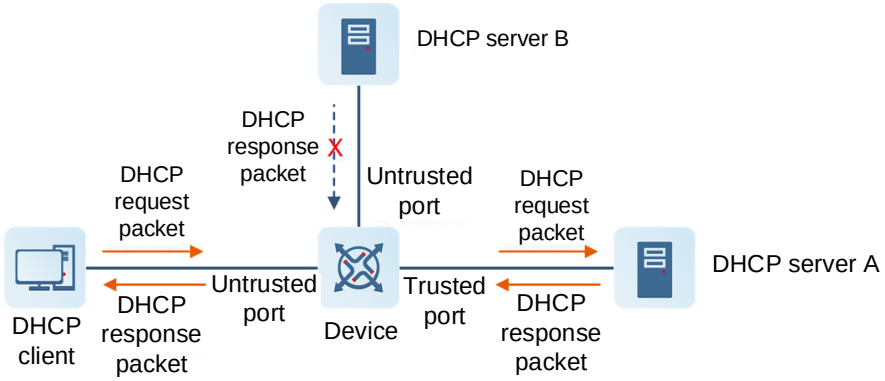
1. Guarding Against DHCP Spoofing

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.

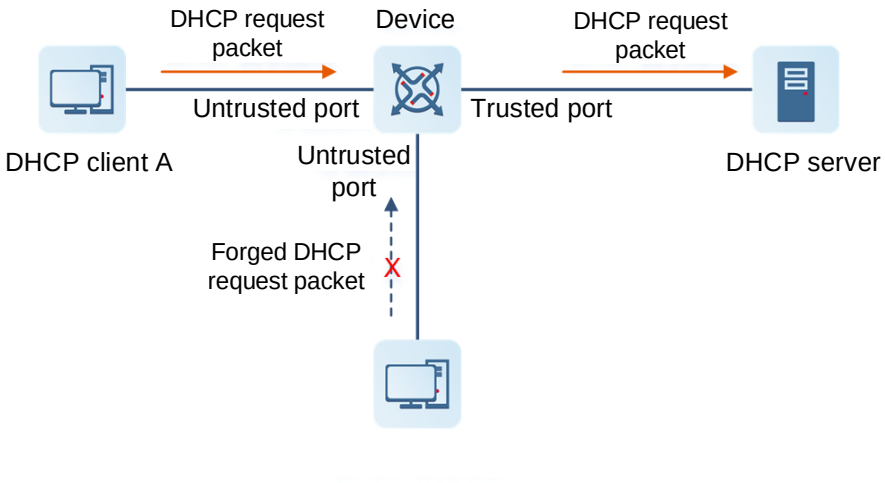
3. Guarding Against Forged DHCP Packets

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.

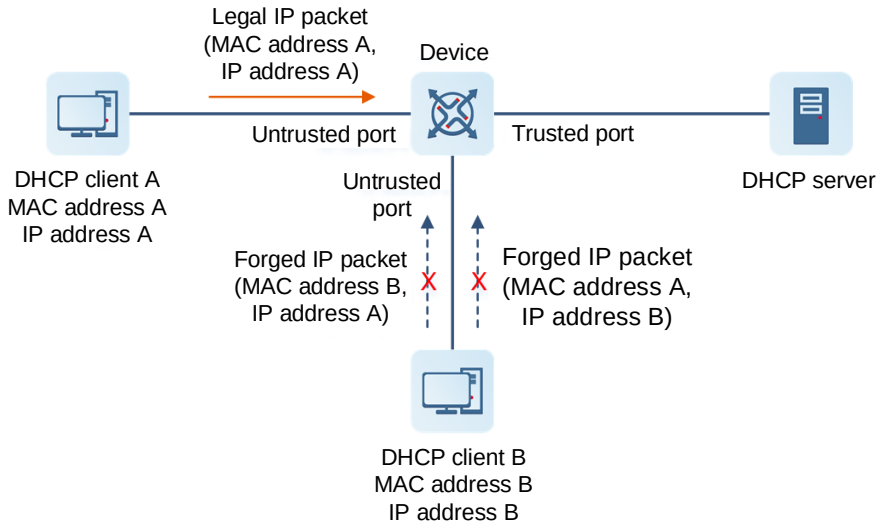
4. Guarding Against IP/MAC Address Spoofing

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".

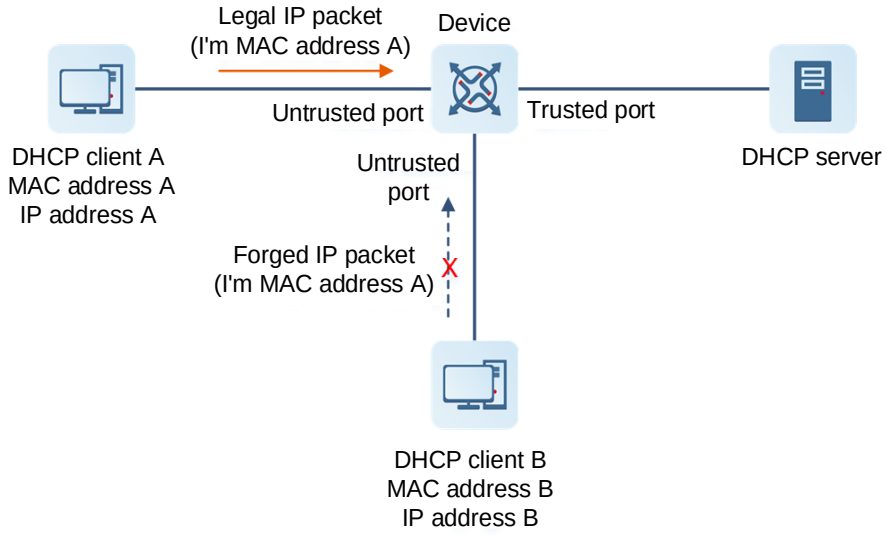
6. Detecting ARP Attacks

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 and L2 APs.
- DHCP snooping and DHCP Relay are mutually exclusive in virtual routing and forwarding (VRF) scenarios.
- A device uses the following rules to process the received DHCP packets:
  - If all interfaces on the device are in the UNTRUST state, the device will discard all the DHCP request and response packets received by the interfaces.
  - If any interface on the device is configured as a trusted interface, the device will use the trusted interface to forward the DHCP request packets received by UNTRUST interfaces, and will discard the DHCP response packets received by UNTRUST interfaces.

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) Enabling the Loose Forward Function for DHCP Snooping
  - k (Optional) Configuring an Interface in the Suppression State
  - l (Optional) Configuring the Maximum Number of Users Bound to a VLAN
  - m (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 copy DHCP packets, generate binding entries based on interaction, check packet validity to filter out unauthorized 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

Run this command to configure the interface connected to an authorized DHCP server as a trusted port. DHCP Response packets received on trusted ports are forwarded normally, while those received on untrusted ports are discarded.

The command is only configured and takes effect on Layer 2 Ethernet interfaces and Layer 2 link aggregation interfaces.

1.5 Disabling DHCP Snooping on a VLAN

1.5.1 Overview

DHCP snooping is enabled on a per-VLAN basis. You can flexibly configure the VLANs on which DHCP snooping is enabled.

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.

Enter the Layer 2 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

Enter the Layer 2 aggregate interface configuration mode.

interface aggregateport *interface-number*

(4) 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

1.7.1 Overview

You can write dynamic user information in the DHCP snooping binding database to the flash memory in real time.

1.7.2 Procedure

(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

1.8.1 Overview

You can write dynamic user information in the DHCP snooping binding database to the flash memory at a scheduled time.

1.8.2 Procedure

(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

1.9.1 Overview

By default, the DHCP snooping feature only forwards BOOTP packets. After this feature is enabled, the DHCP snooping feature snoops BOOTP packets. After a BOOTP client successfully applies for an IP address, the DHCP snooping feature adds the BOOTP client to the static binding database.

1.9.2 Procedure

(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

1.10.1 Overview

You can enable DHCP snooping to support relay request packet processing.

1.10.2 Procedure

(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

1.11.1 Overview

You can enable DHCP snooping to support binding entry migration.

1.11.2 Procedure

(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

1.12.1 Overview

You can enable DHCP snooping to fast age client migration entries.

1.12.2 Procedure

(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 Enabling the Loose Forward Function for DHCP Snooping

1.13.1 Overview

After this function is enabled, when the DHCP snooping binding table is full, new users' DHCP packets can still be forwarded to obtain address information, but DHCP snooping will not add binding entries for those users.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the loose forward function for DHCP snooping.

ip dhcp snooping loose-forward

The loose forward function for DHCP snooping is disabled by default.

1.14 Configuring an Interface in the Suppression State

1.14.1 Overview

You can configure an interface in the suppression state to discard all DHCP packets sent to the interface.

1.14.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.15 Configuring the Maximum Number of Users Bound to a VLAN

1.15.1 Overview

You can configure the maximum number of users bound to a VLAN.

1.15.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.16 Configuring Option 82

1.16.1 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.

1.16.2 Restrictions and Guidelines

Option 82 and DHCP Relay are mutually exclusive.

1.16.3 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) Configure a strategy for processing Option 82.

ip dhcp snooping information option strategy { **drop** | **keep** | **replace** }

The default strategy for processing Option 82 is **replace**; that is, Option 82 in the received DHCP request packets is replaced and then forwarded.

(5) (Optional) Set **Remote ID** to a user-defined string or the host name.

ip dhcp snooping information option format remote-id { **hostname | string** *ascii-string* }

Remote ID in Option 82 is not set to a user-defined string or host name by default.

(6) (Optional) Customize **Remote ID** in Option 82.

ip dhcp snooping information option user-defined remote-id *text*

Customization of **Remote ID** in DHCP Option 82 is disabled by default.

(7) (Optional) Customize **Circuit ID** in Option 82.

ip dhcp snooping information option user-defined circuit-id *text*

Customization of **Circuit ID** in DHCP Option 82 is disabled by default.

(8) (Optional) Configure the format of the MAC address string in the sub-option of DHCP Option 82.

ip dhcp snooping information option user-defined mac-str-format *type*

The user-defined MAC address string is in **H.H.H** format by default.

(9) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(10) (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.

(11) (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.

1.17 Enabling DHCP Snooping Monitoring

1.17.1 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.

1.17.2 Restrictions and Guidelines

The DHCP snooping monitoring and DHCP snooping functions are mutually exclusive.

1.17.3 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.

1.18 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.
show ip dhcp snooping capability	Displays whether DHCP snooping and its features are supported.
show ip dhcp snooping packet [**detail** [*mac-address*]]	Displays packet statistics of DHCP snooping.
show ip dhcp snooping scc-record	Displays security control center (SCC) delivery records.
clear ip dhcp snooping binding [*ipv4-address*] [*mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	Clears all dynamic users in the DHCP snooping database.

1.19 Configuration Examples

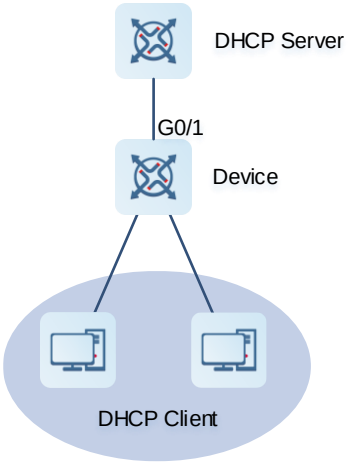
1.19.1 Configuring DHCP Snooping

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
Default                       No           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 0/2
```

6. Configuration Files

Device configuration file

```
hostname Device
!
ip dhcp snooping
!
interface GigabitEthernet 0/1
 ip dhcp snooping trust
!
end
```

1.20 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
1.4.1 Overview 3
1.4.2 Procedure 3
1.5 Configuring Dynamic Domain Name Resolution 3
1.5.1 Overview 3
1.5.2 Restrictions and Guidelines 3
1.5.3 Prerequisites 4
1.5.4 Procedure 4
1.6 Configuring DNS Proxy 4
1.6.1 Overview 4
1.6.2 Prerequisites 4
1.6.3 Procedure 5
1.7 Monitoring 6
1.8 Configuration Examples 6

1.8.1 Configuring Static Domain Name Resolution 6

1.8.2 Configuring Dynamic Domain Name Resolution 8

1.8.3 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 domain name or 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 improves 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.

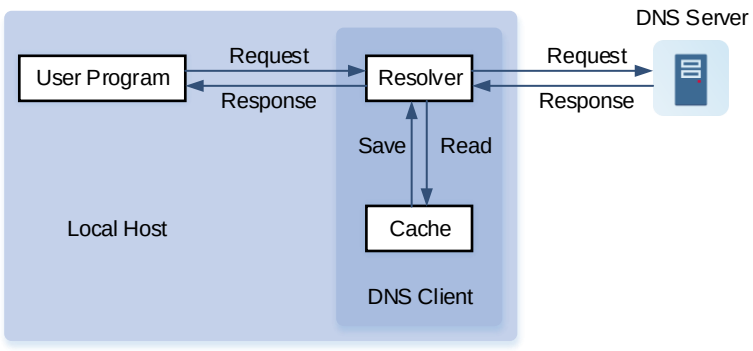
When the application programs access a small number of relatively fixed hosts, the domain name-IP mappings can be configured in advance in the form of static domain name entries. Then, no search request needs to be sent to the DNS server, improving the resolution efficiency.

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 DNS Proxy

1.4 Configuring Static Domain Name Resolution

1.4.1 Overview

Static domain name resolution allows a user to preset the mappings between domain names and IP addresses on a device. The system can find the IP address mapped to a domain name from the device without obtaining the required IP address from a DNS server on the network.

1.4.2 Procedure

(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 [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ipv4-address*

Static mapping between domain names and IPv4 addresses is not configured by default.

(IPv6 network)

ipv6 host [**vrf** *vrf-name*] *host-name* [*telnet-port*] *ipv6-address*

Static mapping between domain names and IPv6 addresses is not configured by default.

1.5 Configuring Dynamic Domain Name Resolution

1.5.1 Overview

Dynamic domain name resolution allows the system DNS resolver to query an external DNS server for the IP addresses mapped to domain names when a user performs domain name operations through applications.

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.

1.5.2 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 an IPv6 DNS query packet will fail to be sent. 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 an IPv4 DNS query packet will fail to be sent.

⚠ Caution

An effective IPv6 address is a unicast address, but it cannot be a local link address or a loopback address.

1.5.3 Prerequisites

The IP address of a DNS server has been obtained.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DNS domain name resolution.

ip domain-lookup [**vrf** *vrf-name*]

DNS domain name resolution is enabled by default.

(4) Configure a DNS server.

(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.

(5) 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 [**vrf** *vrf-name*] **source** *interface-type interface-number*

- Configure the domain name resolution using a specified source IP address.

  (IPv4 network)

  ip domain-lookup [**vrf** *vrf-name*] **source ip** *ipv4-address*

  (IPv6 network)

  ip domain-lookup [**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.

1.6 Configuring DNS Proxy

1.6.1 Overview

DNS proxy is deployed between a DNS server and a PC, and acts as a proxy of a DNS server to process users' DNS domain name resolution requests.

1.6.2 Prerequisites

The IP address of a DNS server has been obtained.

1.6.3 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 domain name and an IPv4 address is configured for the DNS proxy by default.

(IPv6 network)

ip dns proxy host *host-name ipv6-address*

No static mapping between a domain name and an IPv6 address is configured for the DNS proxy 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 source port range is from 55,000 to 58,000.

If the port range is too narrow, the concurrent processing performance of the device is affected. If the port range is too wide, excessive flow table entry resources will be occupied and the egress device needs to adjust the flow table restriction synchronously.

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.

⚠ 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 domain name cache table.
show hosts [*host-name*]	Displays DNS parameters.
debug ip dns	Debugs the DNS function.
clear dns proxy host [*host-name*] | *****]	Clears the dynamic domain name cache table on the DNS proxy.
show dns proxy hosts	Displays DNS parameters on the DNS proxy.
show dns proxy statistics	Display packet statistics on the DNS proxy.
debug dns-proxy	Debugs the DNS proxy.

1.8 Configuration Examples

1.8.1 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 domain 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 the Layer 3 Ethernet interface GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-GigabitEthernet 0/1)# no switchport
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   192.168.10.2       ---
```

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
 no switchport
 ip address 192.168.10.1 24
!
 ip host www.test.com 192.168.10.2
!
```

1.8.2 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)# no switchport
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)
www.dnstest.com           dynamic      192.168.10.2      126
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitEthernet 0/1
 no switchport
 ip address 192.168.10.1 24
!
 ip name-server 192.168.10.2
!
```

1.8.3 Configuring DNS Proxy

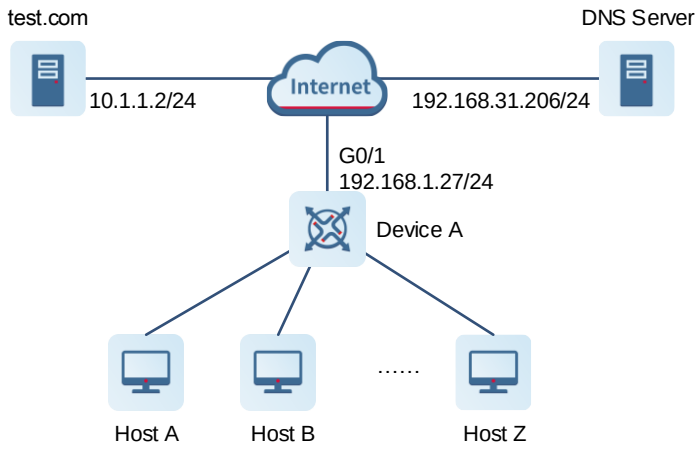
1. Requirements

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 be 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)# no switchport
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
 no switchport
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 18
1.4.3 Configuring an IPv6 Address 18
1.4.4 Configuring the IPv6 MTU for an Interface 19
1.4.5 Configuring the Static IPv6 Path MTU 20
1.4.6 Configuring the Aging Time for the Dynamic IPv6 Path MTU 20
1.4.7 Configuring the IPv6 Fragment Reassembly Function 21
1.4.8 Configuring IPv6 Source Routing 21
1.4.9 Configuring the IPv6 Hop Limit 22
1.4.10 Configuring the Specified Source Address for Sending ICMPv6 Packets 22
1.4.11 Configuring the Transmission Rate of ICMPv6 Error Messages 23
1.4.12 Enabling the Function of Sending Next-Hop Timeout Error Packets 24

1.4.13 Enabling the Function of Sending Destination Unreachable Error Packets.....24
1.5 Configuring IPv6 NDP.....25
1.5.1 Overview.....25
1.5.2 Configuration Task Summary.....25
1.5.3 Configuring a Static Neighbor Entry.....25
1.5.4 Configuring ND Entry Management.....26
1.5.5 Configuring Address Resolution.....28
1.5.6 Configuring NUD.....29
1.5.7 Configuring DAD.....30
1.5.8 Configuring Redirection.....31
1.5.9 Configuring Parameters Related to RA Packets.....31
1.5.10 Configuring ND Logging.....33
1.5.11 Configuring the Interval for ND Packet Rate Statistics Collection.....34
1.5.12 Configuring Local ND Proxy.....34
1.5.13 Configuring the ND Protocol to Allocate Different Prefixes to Different Users.....34
1.5.14 Disabling Dynamic ND Entry Learning.....35
1.5.15 Configuring ND Entry Thresholds for Enabling the Anti-DoS Attack Function.....35
1.5.16 Restraining an Interface from Sending NS Packets to Authenticated VLANs.....36
1.6 Monitoring.....37
1.7 Configuration Examples.....38
1.7.1 Manually Configuring IPv6 Addresses.....38
1.7.2 Enabling Stateless IPv6 Address Auto-configuration.....40

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, multiple 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: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).

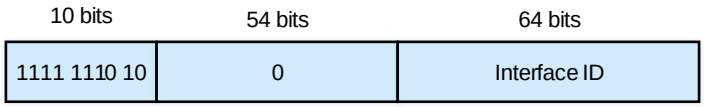
- Loopback address

  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



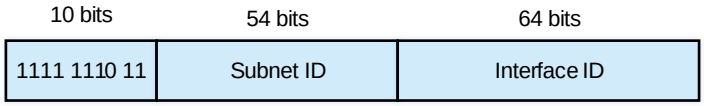
A link-local address is used to number hosts on a single network link. The address identified by the first 10 bits in the prefix is the link-local address. A device will not forward packets in which the source or destination address contains the link-local address. The middle 54 bits of this address 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

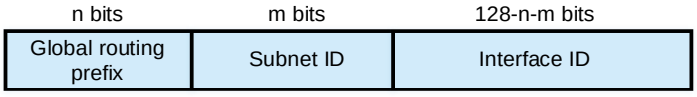


A site-local address can be used to transmit data within a site. A device never forwards packets in which the source or destination address contains a site-local address to the Internet. A site can be assumed as an enterprise's local area network (LAN). Such addresses are similar to IPv4 private addresses 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:

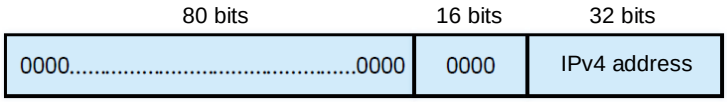
Figure 1-3 Global Unicast Address



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.

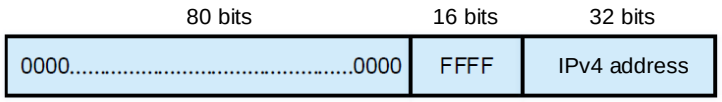
  - The format of an IPv4-compatible IPv6 address is as follows:

Figure 1-4 Format of an IPv4-compatible IPv6 Address



- The format of an IPv4-mapped IPv6 address is as follows:

Figure 1-5 Format of an IPv4-mapped IPv6 Address



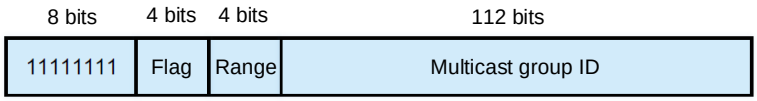
IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. At present, IPv4-compatible IPv6 addresses have been abolished. IPv4-mapped IPv6 addresses are used by IPv6 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



- 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

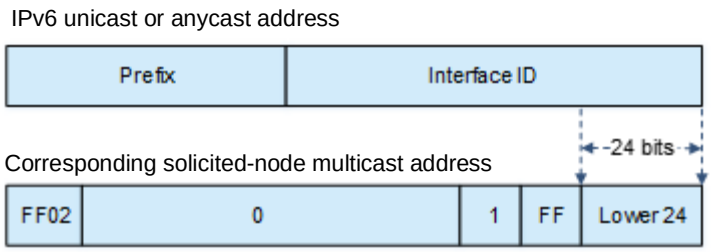
- Multicast group ID field:

  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

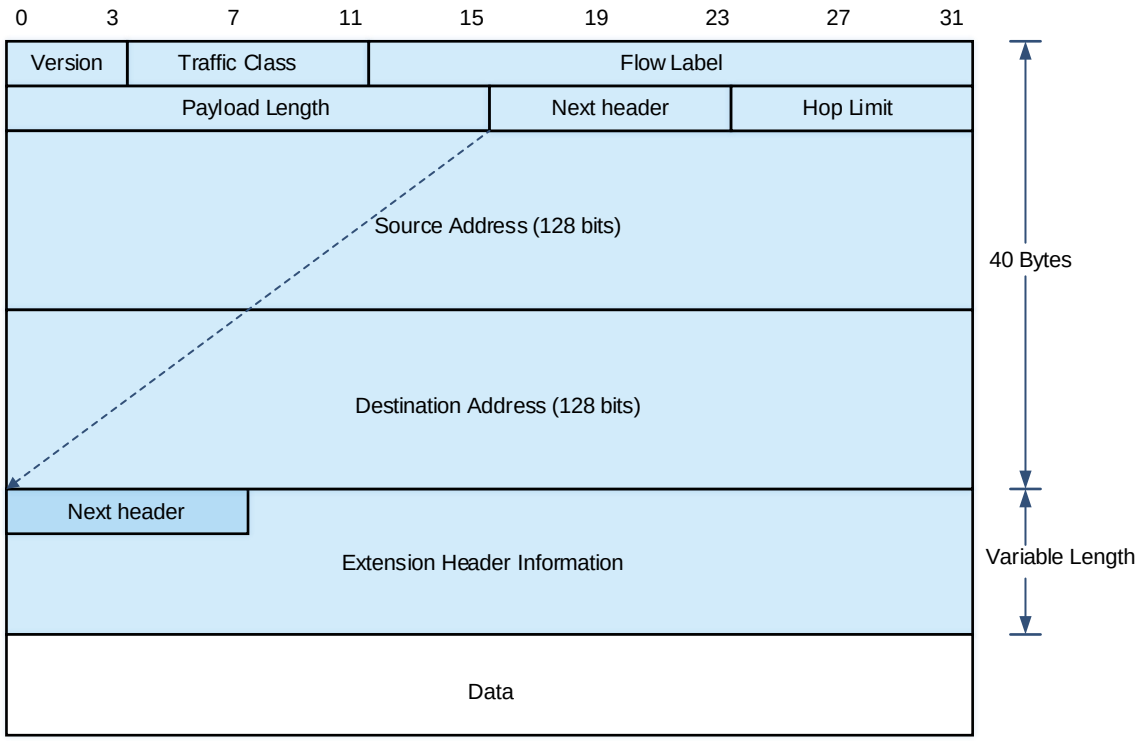
The 64-bit interface ID in an IPv6 address is used to identify a unique interface on the link. This address is a variation of a link-layer address (such as an MAC address) of an interface. This address is generated by inserting a hexadecimal number FFFE after the 24th bit of an MAC address. To make the 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 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

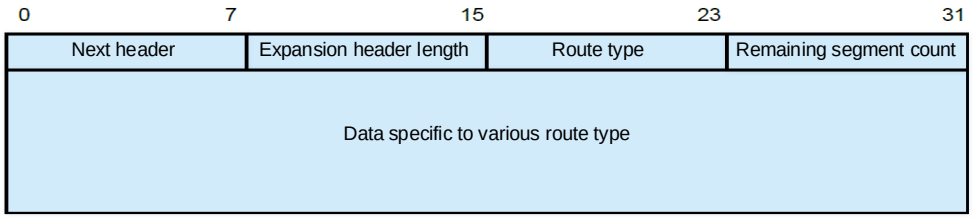
  This extension header indicates the protocol used by the upper layer for data transmission, such as TCP (6) and UDP (17).

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:

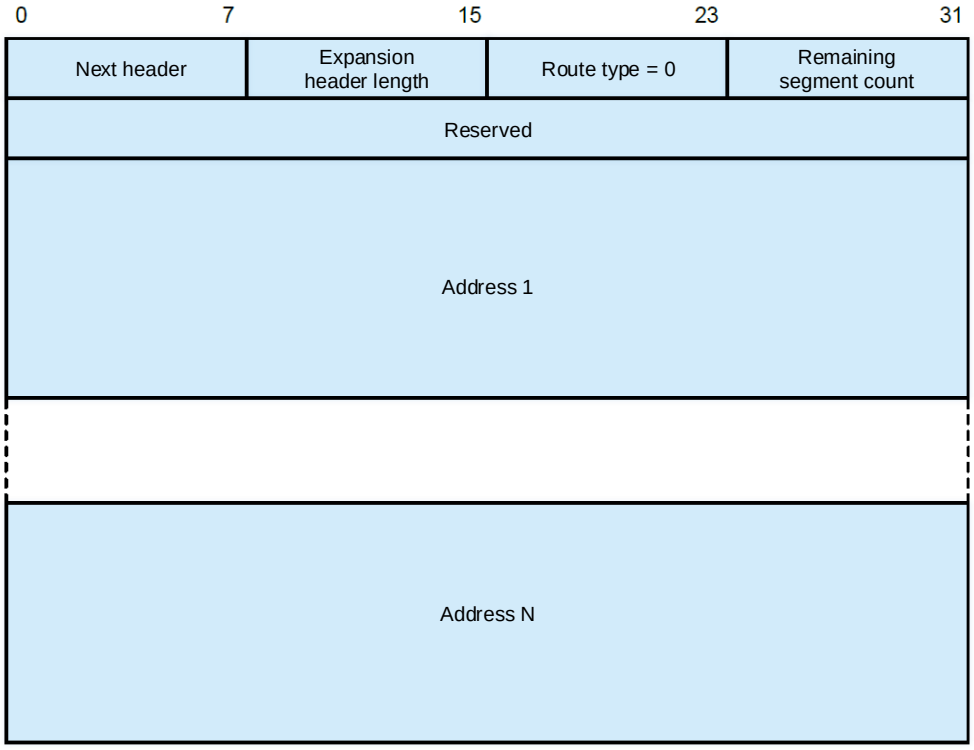
Figure 1-10 IPv6 Routing Header



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.

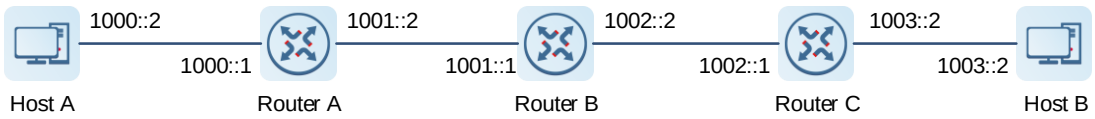
Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. Type 0 routing header is similar to the loose source routing option of IPv4. The format of the Type 0 routing header is as follows:

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**.

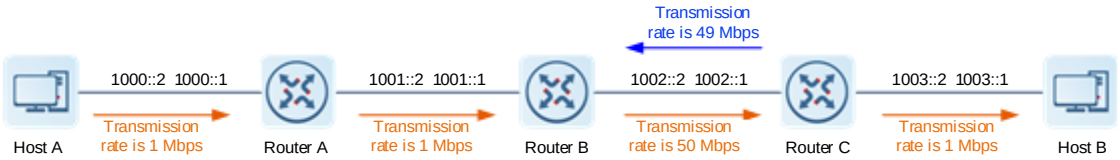
(2) Router A forwards the packet to router B.

(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



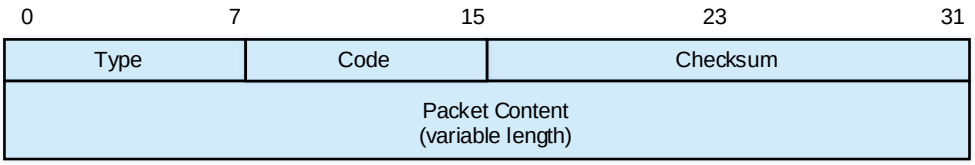
10. IPv6 Hop-limit

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.
  - Code=5, strategy failed.
  - Code=6, routing denied.

- 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

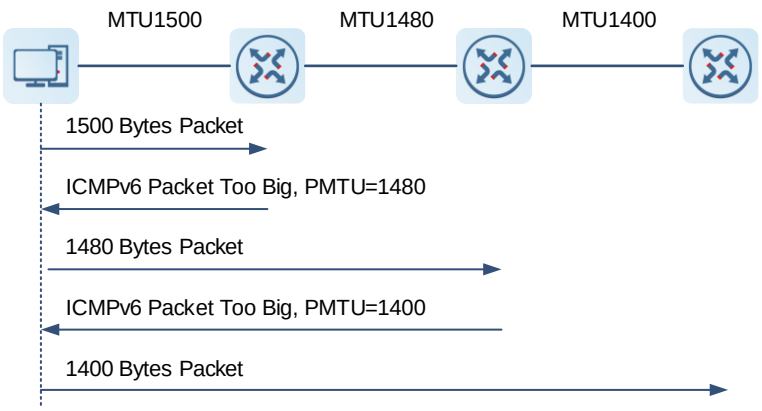
The following describes common informational messages:

- 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.

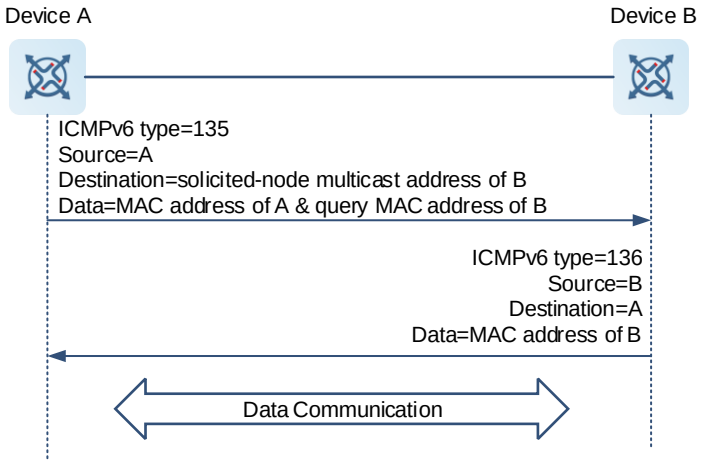
All the above ICMP packets carry one or more options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: **Source Link-Layer Address** option, Type = 1; **Target Link-Layer Address** option, Type = 2; **Prefix Information** option, Type = 3; **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.

- Routing options: Provide IPv6 terminals with specific routing information.

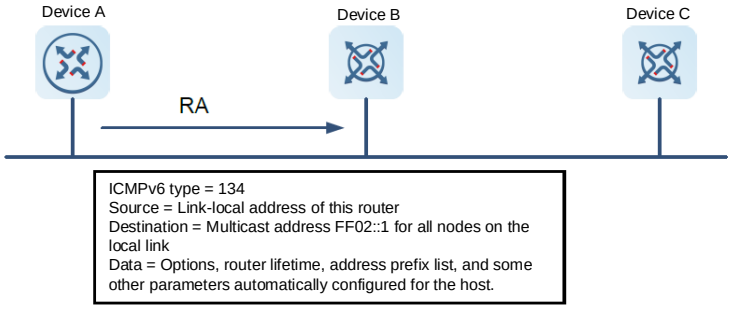
5. Router Discovery

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.

The nodes automatically configure the IPv6 address based on the information obtained from router discovery which is called stateless auto-configuration.

The RA packet sending process during router discovery is shown in the following figure:

Figure 1-17 Router 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
- RFC4191: Default Router Preferences and More-Specific Routes

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 the Static IPv6 Path MTU

(4) (Optional) Configuring the Aging Time for the Dynamic IPv6 Path MTU

(5) (Optional) Configuring the IPv6 Fragment Reassembly Function

(6) (Optional) Configuring IPv6 Source Routing

(7) (Optional) Configuring the IPv6 Hop Limit

(8) 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 (5); (2) Configure an IPv6 address for the interface by referring to Step (6). 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) (Optional) Configure an IPv6 general prefix.

ipv6 general-prefix *prefix-name ipv6-prefix*/*prefix-length*

No IPv6 general prefix is configured by default.

(4) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.
  interface loopback *interface-number*

(5) (Optional) Enable IPv6 on the interface.

ipv6 enable

IPv6 is disabled on an interface by default.

(6) 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.

- 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(4) Configure the IPv6 MTU for the Interface.

ipv6 mtu *bytes*

The MTU value of an IPv6 packet is the same as the value on an interface by default.

1.4.5 Configuring the Static IPv6 Path MTU

1. Overview

IPv6 path MTU refers to the maximum transmission unit on the path to the IPv6 destination address. When a local host sends an IPv6 packet, if there is a path MTU to the destination address and the packet size is greater than the path MTU, the packet needs to be fragmented before it is sent out.

1. Restrictions and Guidelines

When a local host sends an IPv6 packet, it compares the IPv6 MTU of the outbound interface with the path MTU. If the packet size is greater than the smaller value of the two MTUs, the packet will be fragmented based on the smaller value.

2. Procedure

(3) Enter the privileged EXEC mode.
enable

(4) Enter the global configuration mode.
configure terminal

(5) Configure the static IPv6 path MTU.
ipv6 path-mtu [**vrf** *vrf-name*] *ipv6-address value*

The static IPv6 path MTU is not configured by default.

1.4.6 Configuring the Aging Time for the Dynamic IPv6 Path MTU

1. Overview

A device can learn the dynamic path MTU through IPv6 Packet Too Big error packets. The dynamic path MTU has an aging time. Before aging, the learned dynamic path MTU value can only decrease, but cannot increase. In practice, when the network topology changes, routes and paths change, causing that the learned path MTU is smaller than the actual path MTU. Therefore, the path MTU needs to be aged periodically and then relearned.

2. Restrictions and Guidelines

- When the aging time of the dynamic path MTU expires, the dynamic path MTU will be deleted. Before the path MTU is relearned, large IPv6 packets whose sizes exceed the MTU may be discarded by the router during forwarding.

- If the LAN is connected to the Internet through a path with a small MTU and the MTU of this path is the minimum among all paths, you can configure the aging time to be longer or configure it to never age, thus preventing frequent packet loss caused by dynamic path MTU aging every 10 minutes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the aging time for the dynamic IPv6 path MTU.

ipv6 path-mtu age { *age-time* | **infinity** }

The dynamic path MTU ages in ten minutes by default.

1.4.7 Configuring the IPv6 Fragment Reassembly Function

1. Overview

By default, a device reassembles the IPv6 packets sent to the CPU, and then determines whether to forward them or process them locally. This function needs to be disabled if you do not want to reassemble the IPv6 packets sent to the CPU.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable the IPv6 fragment reassembly function.

ipv6 reassemble disable

The IPv6 fragment reassembly function is enabled by default.

1.4.8 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) Enables the device to forward IPv6 packets carrying the routing header.

ipv6 source-route

The device does not forward IPv6 packets carrying the routing header by default.

1.4.9 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.

1.4.10 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.

1.4.11 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 error message.

ipv6 icmp error-interval [too-big] *interval* [*bucket-size*]

Ten messages are transmitted within 100 ms by default.

1.4.12 Enabling the Function of Sending Next-Hop Timeout Error Packets

1. Overview

After the function of sending next-hop timeout error packets is enabled, a device will discard the received IPv6 data packets when the next hop times out due to the specified hop limit and will send ICMPv6 timeout error packets to the source address.

2. Restrictions and Guidelines

Adversaries may send a device a large number of malicious attack packets to make the device exhausted in dealing with the packets and sending next-hop timeout error packets, causing the device's performance degrade. Adversaries may also trace routes of next-hop timeout error packets to obtain the network topology. To avoid this, you can disable the function of sending next-hop timeout error packets.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of sending IPv6 next-hop timeout error packets.

ipv6 hoplimit-expires enable

The function of sending IPv6 next-hop timeout error packets is enabled by default.

1.4.13 Enabling the Function of Sending Destination Unreachable Error Packets

1. Overview

After the function of sending IPv6 destination unreachable error packets is enabled, a device will discard the received IPv6 data packets when detecting that the destination is unreachable and send an ICMPv6 destination unreachable error packet to the source address.

2. Restrictions and Guidelines

Adversaries may send a device a large number of malicious attack packets to make the device exhausted in dealing with the packets and sending IPv6 destination unreachable error packets, causing the device's performance degrade. To avoid this, you can disable the function of sending IPv6 destination unreachable error messages.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of sending IPv6 destination unreachable error packets.

ipv6 unreachables enable

The function of sending IPv6 destination unreachable error packets is enabled 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
- Configuring the ND Protocol to Allocate Different Prefixes to Different Users
- Disabling Dynamic ND Entry Learning
- Configuring ND Entry Thresholds for Enabling the Anti-DoS Attack Function
- Restraining an Interface from Sending NS Packets to Authenticated VLANs

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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *interface-number*

Enter the loopback interface configuration mode.

interface loopback 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) 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) (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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *interface-number*

(4) Enable the interface to learn ND entries via DAD NS packets.

ipv6 nd dad learning enable

By default, a common interface is not allowed to learn neighbor entries through DAD NS packets. A super VLAN interface is allowed to learn neighbor entries through DAD NS packets.

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 sub-VLANs in the super VLAN.

ipv6 nd resolve vlan { *vlan-list* | **none** }

A device sends NS packets to all sub-VLANs in a super VLAN by default.

(5) (Optional) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *interface-number*

(6) Configure the NS packet retransmission interval.

ipv6 nd ns-interval *interval*

The default NS packet retransmission interval on an interface is unspecified when it is to be filled in the RA packets. The default NS packet retransmission interval is 1000 ms when it is used to control the device to send NS packets.

(7) Configure the consecutive transmission count of NS packets.

ipv6 nd ns-times *times*

The consecutive NS packet transmission count is 3 by default. That is, if no NA packet is received, the device sends the NS packet for another consecutive twice.

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.

The **ipv6 nd stale-time** command can be configured in interface or global configuration mode. The setting configured on an interface takes priority over the global setting. That is, if the duration is configured on an interface, the duration configured on the interface applies. Otherwise, the global setting will apply.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(2) (Optional) Configure the duration in which a neighbor keeps in stale state in global configuration mode.
ipv6 nd stale-time *time*

The default duration in which a neighbor keeps in stale state in global configuration mode is one hour.

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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 1 second.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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) (Optional) 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.

(4) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(5) 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.

(6) (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* } | **proxy**] [**no-autoconfig** | **off-link** | **preference** { *high* | **low** | *medium* }] * | **no-advertise**]

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.

(7) (Optional) Configure the hop limit for RA packets.

pv6 nd ra-hoplimit *ra-hoplimit*

The default hop limit of RA packets is 64.

(8) (Optional) Configure the interval for sending RA packets.

ipv6 nd ra-interval { *interval* | **min-max** *min-interval max-interval* }

The default interval for sending packets is 200 seconds. The actual interval will fluctuate around 200 seconds by ±20%.

(9) (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 same as the interface MTU value. The interface MTU value is usually 1500.

(10) 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 priority of the default router in RA packets.
  ipv6 nd ra preference { **high** | **low** | **medium** }

  The priority of the default router in RA packets is **medium** by default.

- Configure routing option information in RA packets.
  ipv6 nd ra route-information *ipv6-prefix* **lifetime** *route-lifetime* [**preference** { **high** | **low** | **medium** }]

  RA packets do not contain routing option information 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*

At most 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 SVI interface configuration mode.

interface vlan *vlan-id*

(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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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 Disabling Dynamic ND Entry Learning

1. Overview

After this function is disabled on an interface, the interface will no longer learn new dynamic ND entries. In this case, you can configure static ND entries.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 link aggregation configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI configuration mode.
  interface vlan *interface-number*

(4) Disable dynamic ND entry learning.

no ipv6 nd learning enable

Dynamic ND entry learning is enabled by default.

1.5.15 Configuring ND Entry Thresholds for Enabling the Anti-DoS Attack Function

1. Overview

When the percentage of the current number of IPv6 ND entries to the maximum number of IPv6 ND entries allowed by a device reaches the configured threshold, the reachability of ND entries in the STALE state is

probed. When the number of IPv6 ND entries of any single MAC address reaches the configured threshold, the reachability of IPv6 ND entries in the STALE state of that MAC address is probed.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the ND entry threshold for enabling the anti-DoS attack function.

ipv6 nd threshold *percent-value*

The ND entry threshold for enabling the anti-DoS attack function is 70 by default.

(4) Configure the ND entry threshold of a single MAC address for enabling the anti-DoS attack function.

ipv6 nd threshold per-mac *value*

The ND entry threshold of a single MAC address for enabling the anti-DoS attack function is 16 by default.

1.5.16 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 SVI interface configuration mode.

interface vlan *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*] [*interface-type interface-number*]	Clears the dynamically learned neighbor entries.
clear ipv6 path-mtu [**vrf** *vrf-name*] [*ipv6-address*]	Clears the dynamic path MTU information of the public network instance or a specified VRF instance.
clear ipv6 path-mtu all	Clears all dynamic path MTUs.
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-packet [**interface** *interface-type interface-number*] **statistics**	Displays the statistics on IPv6 ND packets.
show ipv6 nd ra dns search-list	Displays the DNSSL option in RA packets and the suppression status and interface for configuring the DNSSL option.
show ipv6 nd ra dns server	Displays the recursive DNS server address provided by the RDNSS option in RA packets and the suppression status and interface for configuring the RDNSS option.
show ipv6 neighbors [**vrf** *vrf-name*] **statistics** [**all**]	Displays the statistics on IPv6 neighbor tables.
show ipv6 packet statistics [*interface-type interface-number* | **total**]	Displays the statistics on IPv6 packets.
show ipv6 neighbors [[**vrf** *vrf-name*] [*interface-type interface-number*] [*ipv6-address*] | [**verbose**] [*ipv6-address*] | **static**]	Displays neighbor information.
show ipv6 neighbor statistics per-mac [*interface-type interface-number*] [*mac-address*]	Displays the number of ND entries corresponding to each MAC address.
show ipv6 path-mtu [**vrf** *vrf-name*] [*ipv6-address* | **dynamic** | **static**]	Displays the path MTU information.
show ipv6 path-mtu statistics	Displays the path MTU statistics.

Command	Purpose
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.

1.7 Configuration Examples

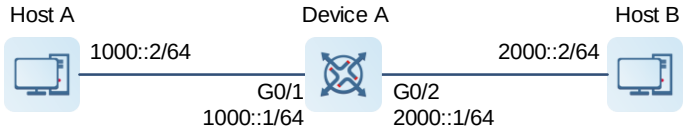
1.7.1 Manually Configuring IPv6 Addresses

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)# no switchport
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)# no switchport
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::2/64.

Set the IPv6 address of host B to 2000::2/64.

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
no switchport
ipv6 enable
ipv6 address 1000::1/64
no ipv6 nd suppress-ra
!
interface gigabitethernet 0/2
no switchport
ipv6 enable
ipv6 address 2000::1/64
no ipv6 nd suppress-ra
!
```

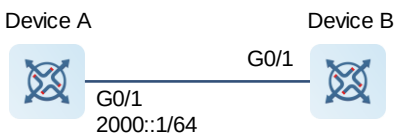
1.7.2 Enabling Stateless IPv6 Address Auto-configuration

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)# no switchport
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)# no switchport
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
no switchport
ipv6 enable
ipv6 address 2000::1/64
no ipv6 nd suppress-ra
!
```

- Device B configuration file

```
hostname DeviceB
!
interface gigabitEthernet 0/1
no switchport
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 15
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 18
1.8.3 Procedure (Global Configuration Mode) 18
1.8.4 Procedure (Interface Configuration Mode) 18
1.9 Monitoring 18
1.10 Configuration Examples 20
1.10.1 Dynamically Assigning IPv6 Addresses 20
1.10.2 Dynamically Assigning IPv6 Address Prefixes 22
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 device applies for a prefix from an upper-layer network device, and the upper-layer network device assigns a proper address prefix to the lower-layer network device. The lower-layer network device 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

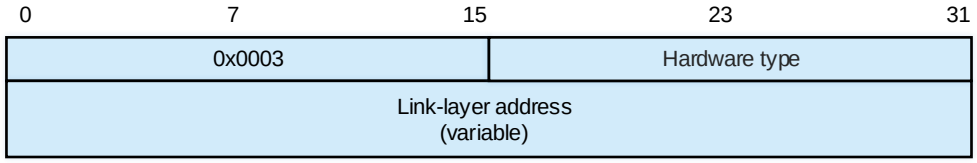
A DHCP Unique Identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, relay, or server). It is used for mutual authentication during DHCPv6 message exchanges.

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.

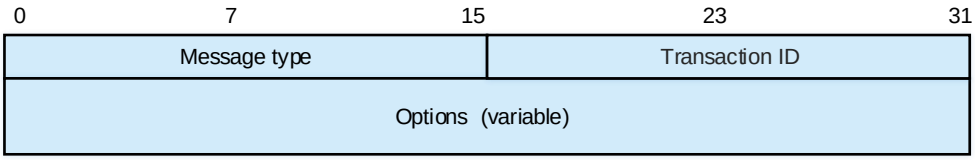
Note

- Ruijie devices serving as DHCPv6 servers do not support RECONFIGURE packets.
- Ruijie devices serving as DHCPv6 servers 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

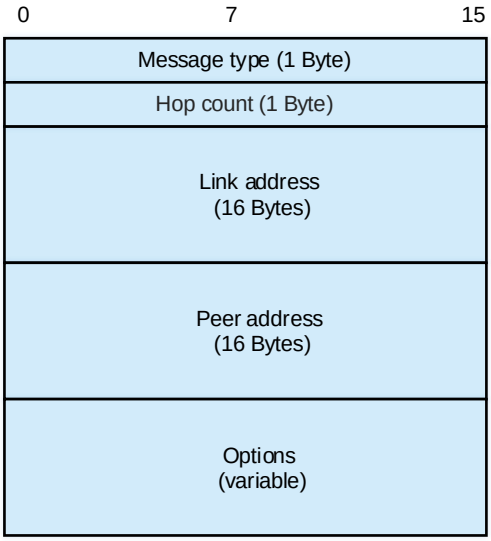
Figure 1-2 Format of Packets Exchanged Between a DHCPv6 Client and a DHCPv6 Server



- **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.

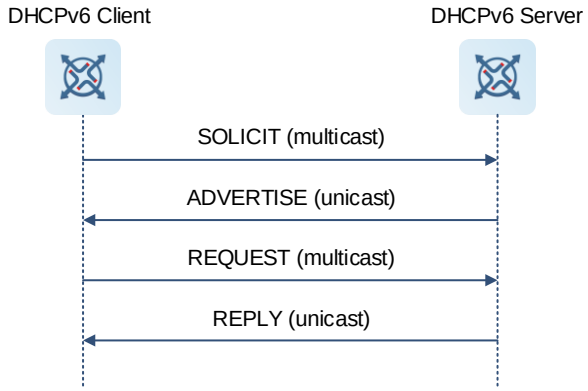
1. Principles

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.

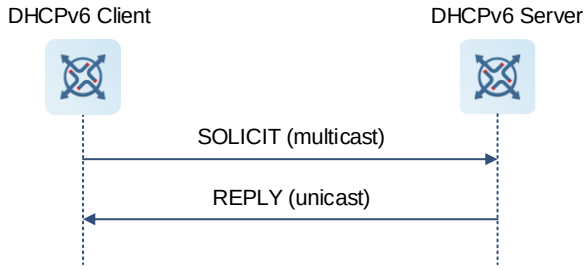
(3) The DHCPv6 client may receive the ADVERTISE messages from multiple DHCPv6 servers. Generally, the DHCPv6 client selects the server from which it first receives the ADVERTISE message as the DHCPv6 server. Then, the DHCPv6 client sends a REQUEST message with the destination address FF02::1:2 and destination 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



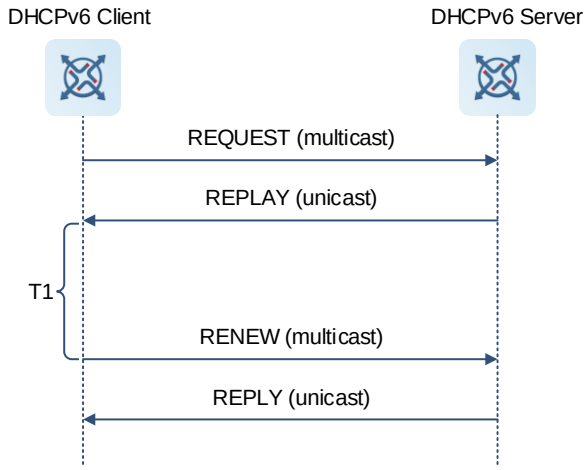
(1) A DHCPv6 client sends a SOLICIT message with the destination address FF02::1:2 and destination port 547 on the local link to request an address, a prefix, and configuration parameters. The SOLICIT message contains the **Rapid Commit** option.

(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.

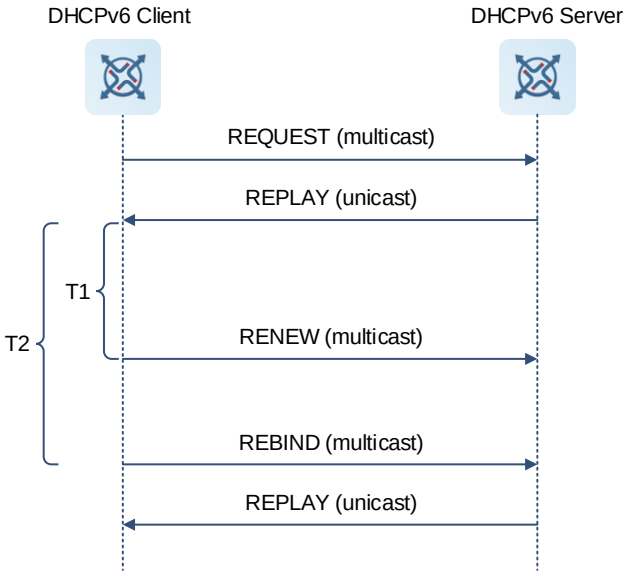
Figure 1-6 Update



(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



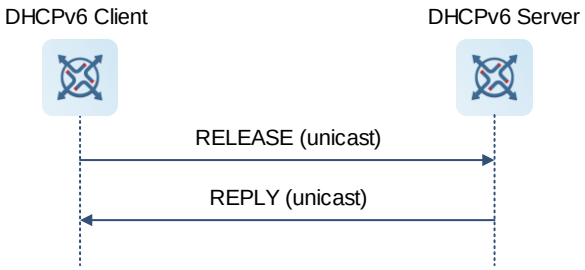
(1) If no response is received within T2 after the DHCPv6 client sends a RENEW message to the DHCPv6 server, the DHCPv6 client sends a REBIND multicast message to the DHCPv6 server for rebinding the address and prefix.

(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

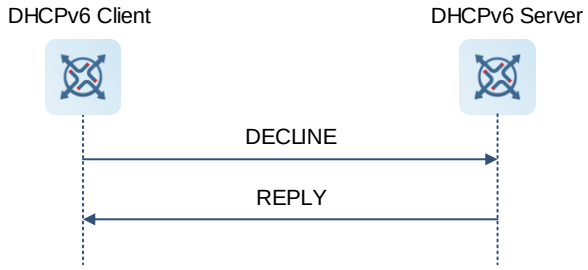
(1) The DHCPv6 client sends a CONFIRM message to the DHCPv6 server on the new link to check whether the original address is still available.

(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 **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.

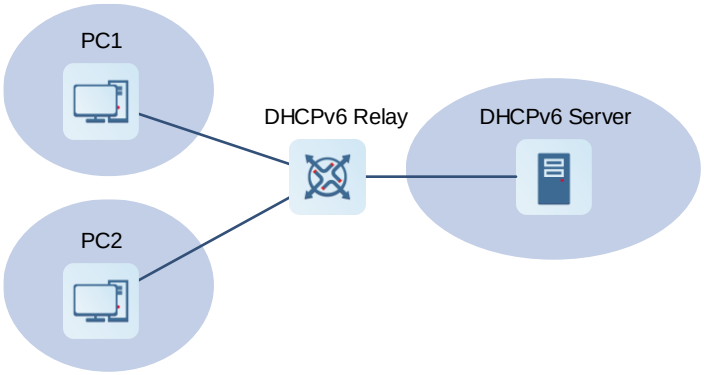
(3) The DHCPv6 client checks whether information provided in the REPLY message is consistent with configuration parameters requested in the INFORMATION-REQUEST message. If yes, the DHCPv6 client performs network configuration based on parameters provided in the REPLY message. Otherwise, it ignores the 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

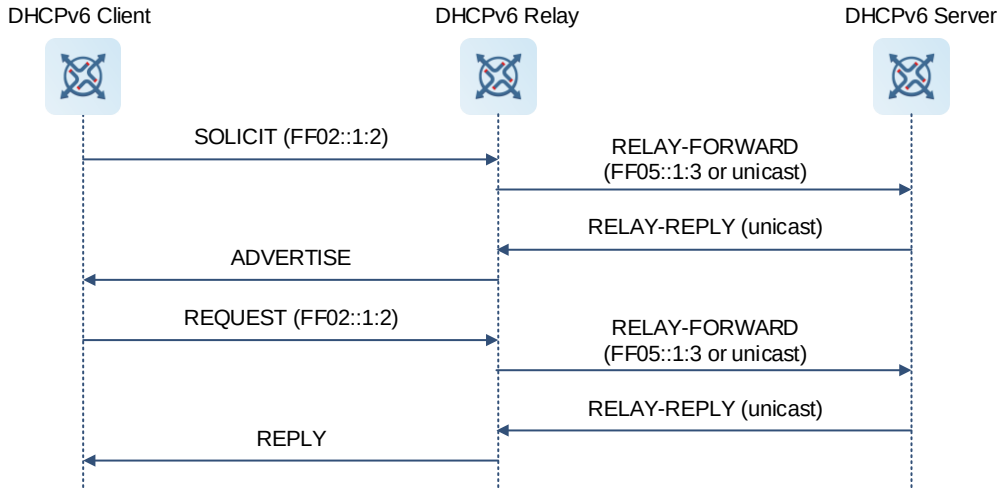
enabling a DHCPv6 client to send packets to a DHCPv6 server on a different link. A DHCP relay agent is often deployed on the link where a DHCPv6 client resides. It is used to forward interaction packets between the DHCPv6 client and a DHCPv6 server. The DHCP relay agent is transparent to the DHCPv6 client.

Figure 1-12 DHCPv6 Relay Agent



2. Principles

Figure 1-13 Packet Exchange Among a DHCPv6 Client, DHCPv6 Relay Agent, and DHCPv6 Server



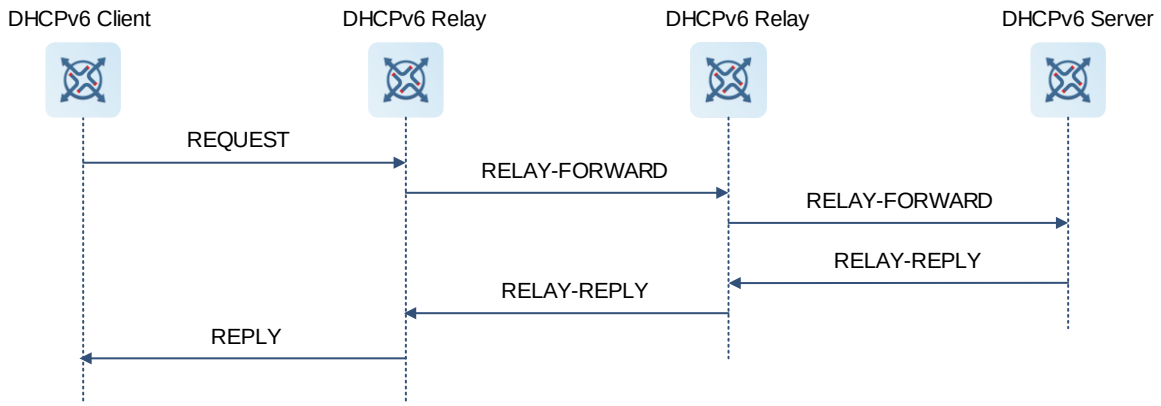
(1) When receiving a SOLICIT or REQUEST message from the DHCPv6 client, a DHCPv6 relay agent creates a RELAY-FORWARD message. This message contains the original message from the DHCPv6 client and multiple options added by the relay agent. Then, the DHCP relay agent sends the RELAY-FORWARD message to 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
- Configuring the DHCPv6 relay
  a Configuring the DHCPv6 Relay
  b (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 ipv6-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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *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-name*

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.

- When a Layer 3 interface is added to or removed from VRF, the existing destination address or interface of DHCPv6 relay will be deleted. After the Layer 3 interface is added to or removed from VRF, enable the DHCPv6 relay function and specify the destination address or interface according to specific requirements.
- When VRF is deleted, the destination address or interface of DHCPv6 relay on the Layer 3 interface added to the VRF will be deleted.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *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** } { *interface-type interface-number* | *ipv6-address* }

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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *interface-number*

(4) Configure the source interface designation function.

ipv6 dhcp relay source { **source-ip-address** | **gateway-address** } { *interface-type interface-number* | *ipv6-address* }

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.
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 dhcp server status	Displays status of a DHCPv6 server.

Command	Purpose
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

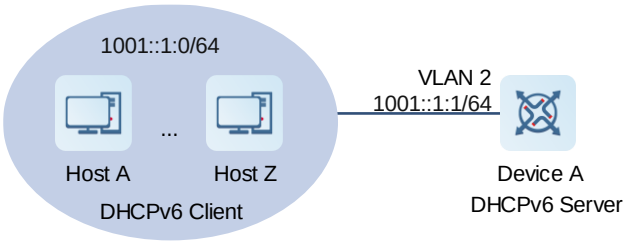
1.10.1 Dynamically Assigning IPv6 Addresses

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.

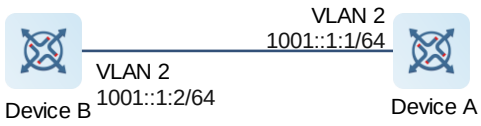
1.10.2 Dynamically Assigning IPv6 Address Prefixes

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.

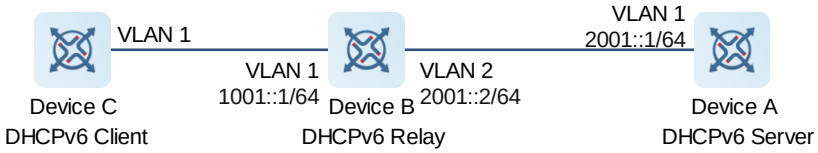
1.10.3 Configuring DHCP Relay

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 Configuration Task Summary 1
1.4 Configuring DHCPv6 Client to Request an IPv6 Address 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 2
1.4.3 Procedure 2
1.5 Configuring DHCPv6 Client to Request an IPv6 Prefix 2
1.5.1 Overview 2
1.5.2 Restrictions and Guidelines 2
1.5.3 Procedure 3
1.6 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.
- Configuring a DHCPv6 client to request an IPv6 address and configuring a DHCPv6 client to request an IPv6 prefix are mutually exclusive.

1.3 Configuration Task Summary

DHCPv6 client configuration includes the following tasks:

- Configuring DHCPv6 Client to Request an IPv6 Address

- Configuring DHCPv6 Client to Request an IPv6 Prefix

1.4 Configuring DHCPv6 Client to Request an IPv6 Address

1.4.1 Overview

Configure a device as a DHCPv6 client to automatically request an IPv6 address 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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

interface vlan *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**]

Both the DHCPv6 Client function and IA_NA address requesting are disabled by default.

(5) (Optional) Configure the stateless service.

ipv6 nd other-config-flag

The stateless service is not configured by default.

1.5 Configuring DHCPv6 Client to Request an IPv6 Prefix

1.5.1 Overview

Configure a device as a DHCPv6 client to automatically request an IPv6 prefix or related parameters from a DHCPv6 server.

1.5.2 Restrictions and Guidelines

The DHCPv6 Client function can be configured only on L3 interfaces.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *interface-number*

(4) Enable the DHCPv6 Client function to request an IPv6 address prefix.

ipv6 dhcp client pd *prefix-name* [**rapid-commit**]

IPv6 address prefix requesting is not configured on a DHCPv6 client 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 **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 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 5
1.1.4 Protocols and Standards 8
1.2 Restrictions and Guidelines 8
1.3 Configuration Task Summary 8
1.4 Configuring Basic DHCPv6 Snooping Functions 8
1.4.1 Overview 8
1.4.2 Procedure 8
1.5 Configuring Optional DHCPv6 Snooping Functions 9
1.5.1 Overview 9
1.5.2 Procedure 9
1.6 Configuring Option 18 or 37 9
1.6.1 Overview 9
1.6.2 Procedure 9
1.7 Monitoring 10
1.8 Configuration Examples 11
1.8.1 Configuring Basic DHCPv6 Snooping Functions 11
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 devices, 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 authorized 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

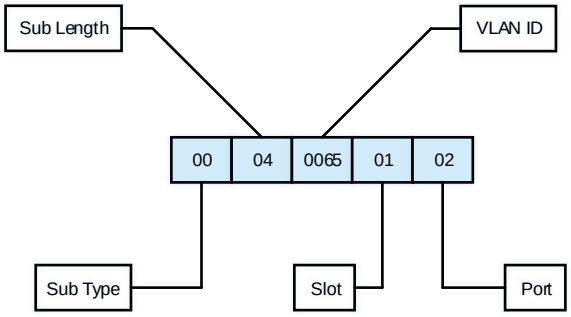
Some network administrators want to assign and manage IP addresses based on information about the network devices connected user clients (that is, client locations). To meet this requirement, a device with DHCPv6 Snooping enabled adds related network device information to DHCPv6 request packets by using 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 and L2 APs. 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.

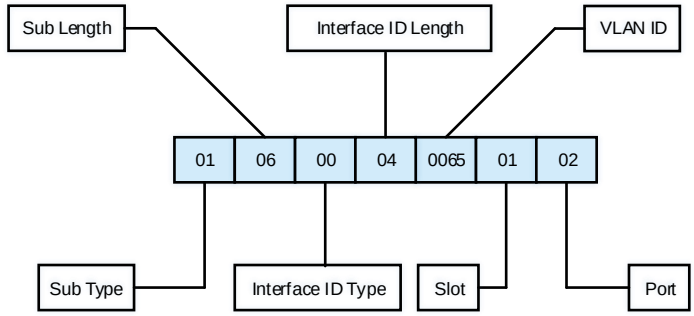
Figure 1-1 Standard Padding Format of Interface ID



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**.

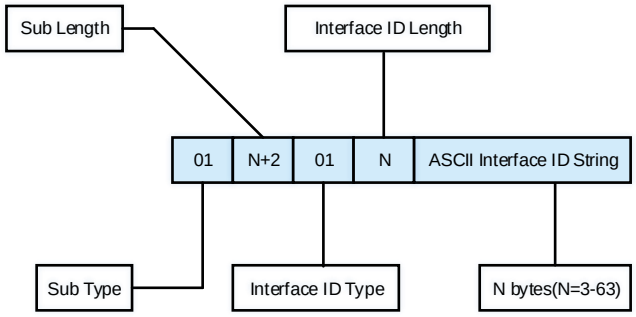
The following figure shows the default padding content in extended padding format.

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

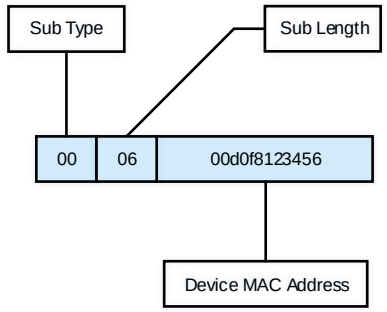


- Option 37: Remote ID

  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

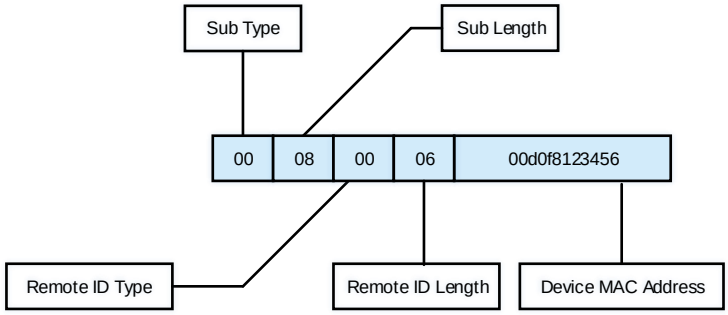


If user-defined padding content is required, use the extended padding format. In extended padding format, the padding content can be the default padding content or extended padding content. To distinguish between different padding content, a 1-byte content type field and a 1-byte content length field 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**.

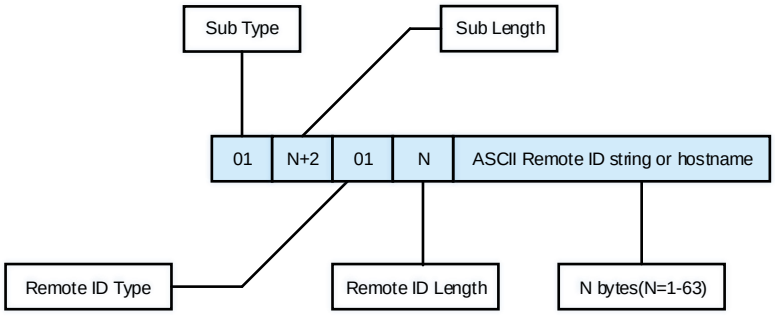
The following figure shows the default padding content in extended padding format.

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 or L2 AP. 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 Gi0/10, the port number is 10. If the AP name is AP 11, the port number is 11.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.

1.1.3 Applications

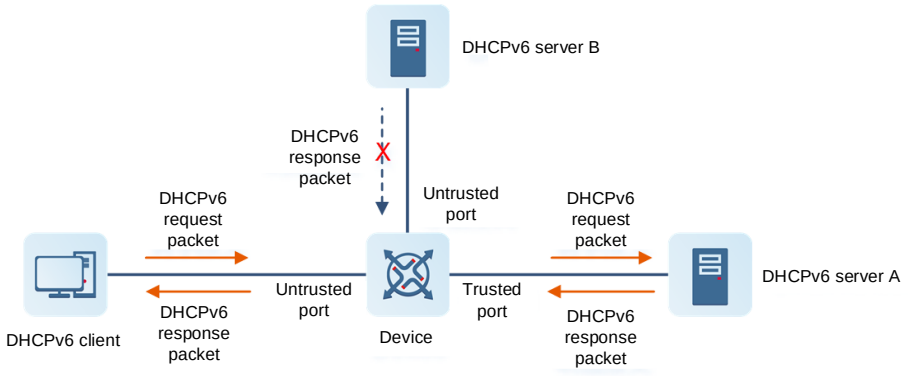
1. Guarding Against DHCPv6 Spoofing

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.

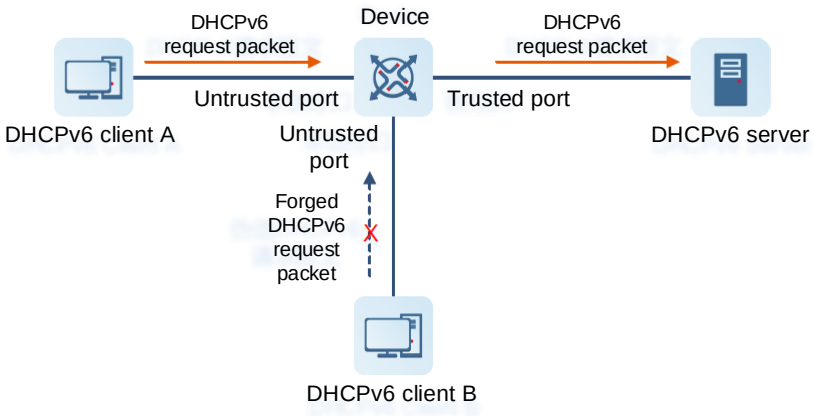
- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server A is configured as a DHCPv6 trusted port to forward response packets.
- The rest ports on Device are configured as DHCPv6 untrusted ports to filter response packets.

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.

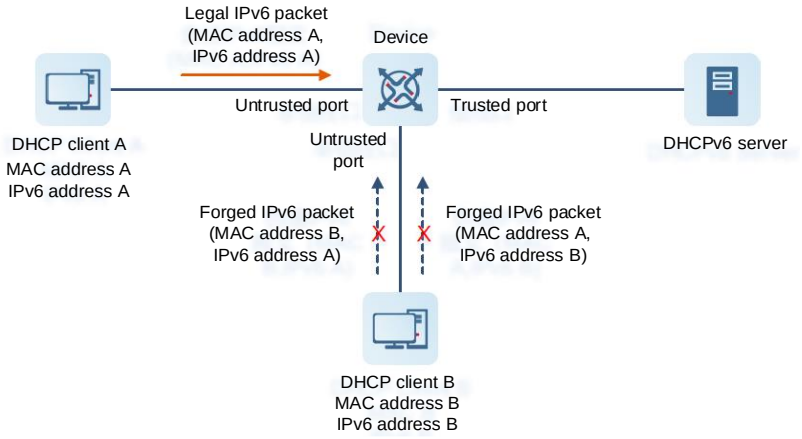
3. Guarding Against IPv6/MAC Address Spoofing

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 and L2 APs.
- 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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

1.5.1 Overview

You can configure optional DHCPv6 Snooping functions, including disabling DHCPv6 Snooping for a specified VLAN, writing all dynamic user information in a DHCPv6 Snooping binding database to a flash memory, and filtering all DHCPv6 request packets on an interface.

1.5.2 Procedure

(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

1.6.1 Overview

After Option 18 or 37 is added to DHCPv6 request packets, the DHCPv6 server can obtain more user information based on the content in Option 18 or 37 and assign IP addresses to users more accurately.

1.6.2 Procedure

(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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 [*mac-address*] [*ipv6-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	Displays dynamic user information in the DHCPv6 Snooping binding database.

Command	Purpose
show ipv6 dhcp snooping prefix [*mac-address*] [*ipv6-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	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 [*mac-address*] [*ipv6-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	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 ipv6 dhcp snooping ipv6 event	Debugs DHCPv6 Snooping events.
no debug ipv6 dhcp snooping ipv6 event	Disables debugging of DHCPv6 Snooping events.
debug ipv6 dhcp snooping ipv6 packet	Debugs DHCPv6 Snooping packets.
no debug ipv6 dhcp snooping ipv6 packet	Disables debugging of DHCPv6 Snooping packets.

1.8 Configuration Examples

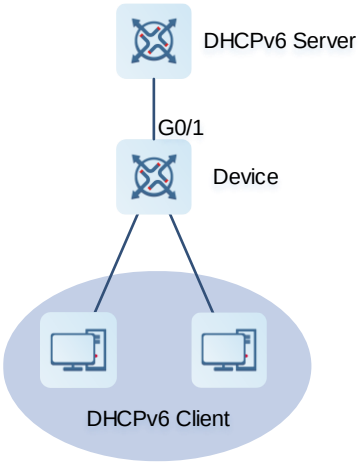
1.8.1 Configuring Basic DHCPv6 Snooping Functions

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: 2
NO.    MAC Address     IPv6 Address                    Lease(sec)   VLAN  Interface
```

```
-----  --------------  --------------------------------  -----------  ----
--------------------
1     fa16.3e42.7a7b  1001::3                           86393       1
GigabitEthernet 0/2
2     fa16.3e4a.b7c8  1001::4                           85807       1
GigabitEthernet 0/3
```

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 6
1.2 Configuration Task Summary 6
1.3 Configuring Basic ND Snooping Functions 6
1.4 Configuring ND Guard 7
1.5 Configuring ND Logging 8
1.6 Configuring Fast Station Movement Through the Port in the ND Snooping Binding Entry 8
1.6.1 Overview 8
1.6.2 Procedure 8
1.7 Configuring ND Snooping Loose Mode 9
1.7.1 Overview 9
1.7.2 Restrictions and Guidelines 9
1.7.3 Procedure 9
1.8 Monitoring 9
1.9 Configuration Examples 10
1.9.1 Configuring ND Guard 10

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

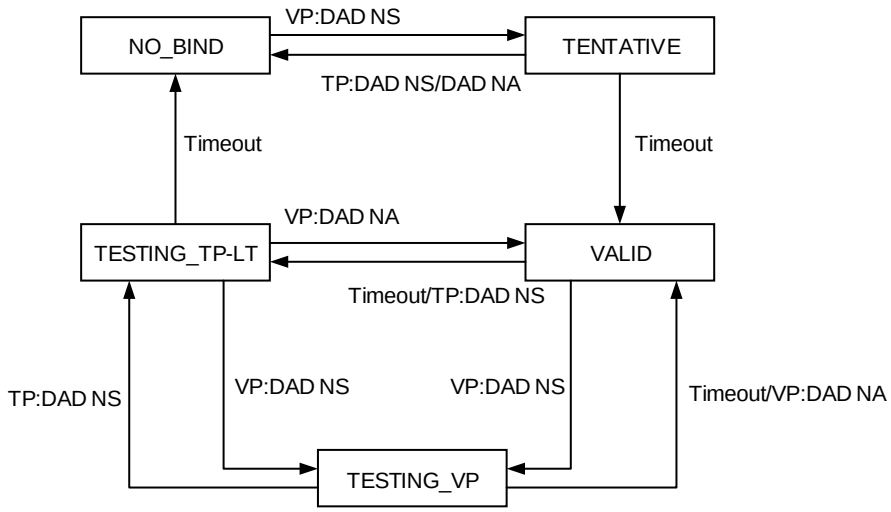
The ND Snooping entries are created by listening to the Duplicate Address Detection (DAD) NS packets, and the table entry content includes the source IPv6 addresses, source MAC addresses, VLANs to which the packets belong, inbound interfaces, and other information of the packets. ND Snooping entries have five states:

- NO_BIND: This is the initial state of binding entries for any access device. When the component is just started, all entries are in this state by default, unless the component loads the binding entries in other ways (for example, the component has exited abnormally and recovered with backup data).
- TENTATIVE: The device has received a DAD NS packet and is waiting for a collision response.
- VALID: The binding entry has been verified and can be used as the basis for filtering.
- TESTING_VP: If a DAD NS packet is received on the validating port (untrusted port) and the source address of the packet conflicts with the binding entry recorded by the current interface, the device enters the probe state. The device needs to determine whether users have moved, other users are statically configuring addresses, or there is an attack.
- TESTING_TP-LT: Entries enter this state in two situations: 1. When a DAD NS packet is received on the trust port (the destination address is the same as the IP address of the binding entry), the device needs to determine whether the user is moved to another switch or an attack occurs. 2. When the lease of a binding entry is about to expire, the device needs to determine whether the user does not send packets because of silence or the user has moved. If the user is in silence state, the entry is retained; if the user has moved, the

entry is removed.

Figure 1-1 shows the status transition. In the figure, TP is the trusted port and VP is the validating port.

Figure 1-1 State Machine of ND Snooping Entries



- Entry creation mechanism

  a. The initial state of an ND Snooping entry is **NO_BIND**. When receiving a DAD neighbor solicitation (NS) packet from an unknown source address on an untrusted port, the device creates an ND Snooping entry in **TENTATIVE** state.

  b. The device sends a specified number of DAD NS packets to ND Snooping trusted ports for snooping.

  c. The entry state is changed depending on whether a neighbor advertisement (NA) response is received within the **TENTATIVE** state timeout time:

  If no NA response is received within the specific period after the last NS packet is sent, no conflicted addresses exist on the local area network (LAN). In this case, the ND Snooping entry is changed to the **VALID** state.

  If an NA packet is received within the specific period after the first NS packet is sent, conflicted addresses exist on the LAN. In this case, the device deletes the ND Snooping entry.

- Entry migration mechanism

  Entry migration includes the following types:

  - Intra-device migration

    a. When the device receives a DAD NS packet with the same source address (target IP address) as an existing ND Snooping entry from an ND Snooping untrusted port on the same VLAN, the entry state is changed to **TESTING_VP**.

    b. The device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping.

    c. The entry state is changed depending on whether an NA response is received within the **TESTING_VP** state timeout time:

If no NA response is received within the specific period after the last NS packet is sent, 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 on an untrusted port within the specific period 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

  a. When the device receives a DAD NS packet with the same source address (target IP 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.

  b. The device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping.

  c. The entry state is changed depending on whether an NA response is received within the **TESTING_TP-LT** state timeout time.

  If no NA packet is received within the specific period after the last packet is sent, 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 on an untrusted port within the specific period after the first NS packet is 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

  a. If no ND packet is received within the **VALID** state timeout time since the last update of an ND Snooping entry, the ND Snooping entry is changed to the **TESTING_TP-LT** state.

  b. The device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping.

  c. The entry state is changed depending on whether an NA response is received within the **TESTING_TP-LT** state timeout time.

  If no NA packet is received within the specific period after the last NS packet is sent, the original user is disconnected from the inbound port. The device deletes the ND Snooping entry.

  If an NA packet is received on an untrusted port within the specific period after the first NS packet is sent, 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.

- Fast station movement through the port in the ND Snooping binding entry

  When a device migrates, the source port of ND packets becomes inconsistent with the port in the ND Snooping entry. In this case, the device sends a DAD NS packet to the port in the ND Snooping entry to check whether the user still exists. If no DAD_NA packet is received within a period of time, the device updates the entry. This process interrupts communication between the user and the device for about one second. After fast station movement through the port in the ND Snooping binding entry is enabled (by the **ipv6 nd snooping fast station-move** command), a device will not perform a check but directly update the ND Snooping entry when the source port of the received ND packet is inconsistent with the port in the ND

Snooping entry, but the IP address, VLAN, and MAC address are all consistent. Fast station movement through the port in the ND Snooping binding entry can shorten the communication interruption time to about 100 milliseconds during device migration, thereby avoiding a large amount of traffic loss.

- ND Snooping loose mode

  After some terminals (such as MacBook) have obtained IPv6 addresses through DHCPv6 for a period of time, the terminals may not reply to DAD_NS packets. The MAC entry aging time is used to indicate the aging time of IPv6 entries for the same MAC address. When ND packets corresponding to any IPv6 entry for this MAC address are received, the MAC entry aging time is updated. Before the MAC entry aging time expires, ND Snooping does not age the IPv6 entries associated with this MAC address. After the MAC entry aging time expires, ND Snooping sends a probe packet to only the local address of the link. If no reply is returned, the terminal is considered offline. This prevents traffic interruption caused because ND Snooping mistakenly considers that the terminal is offline, and then deletes the ND Snooping entry.

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. 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 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 Layer 2 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

(4) (Optional) Configuring Fast Station Movement Through the Port in the ND Snooping Binding Entry

(5) (Optional) Configuring ND Snooping Loose Mode

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-id* | *vlan-range* }

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 for binding entries is 1024 by default.

(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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

(11) (Optional) Configure the maximum number of ND Snooping binding entries for a single MAC address.

ipv6 nd snooping threshold per-mac *number*

The maximum number of ND Snooping binding entries is not configured for a single MAC address 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 Configuring Fast Station Movement Through the Port in the ND Snooping Binding Entry

1.6.1 Overview

After fast station movement through the port in the ND Snooping binding entry is enabled, a device will not perform a check but directly update the ND Snooping entry when the source port of the received ND packet is inconsistent with the port in the ND Snooping entry, but the IP address, VLAN, and MAC address are all consistent.

1.6.2 Procedure

(2) Enter the privileged EXEC mode.

enable

(3) Enter the global configuration mode.
configure terminal

(4) Enable fast station movement through the port in the ND Snooping binding entry.
ipv6 nd snooping fast station-move

Fast station movement through the port in the ND Snooping binding entry is disabled by default.

1.7 Configuring ND Snooping Loose Mode

1.7.1 Overview

After some terminals (such as MacBook) have obtained IPv6 addresses through DHCPv6 for a period of time, the terminals may not reply to DAD_NS packets (duplicate address check) sent by other terminals. As a result, ND Snooping may mistakenly consider that the terminals are offline and then delete corresponding ND Snooping entries. With the ND Snooping loose mode, aging probing is performed after the MAC aging time expires. Only when a terminal is offline at all IPv6 addresses, or no ND packet is received from a specific IPv6 address in multiple consecutive lease periods, the ND Snooping entries corresponding to the specific IPv6 address are deleted.

1.7.2 Restrictions and Guidelines

ND Snooping performs aging probing on all entries in loose mode. In ND Snooping loose DHCP mode, when the source of an entry is DHCPv6 Snooping, no aging probing is performed on the entry.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Configure ND Snooping loose mode.
ipv6 nd snooping loose-state [**loose-dhcp**]

The ND Snooping loose mode is not configured by default.

(4) (Optional) Configure the number of offline terminal probing times in ND Snooping loose mode.
ipv6 nd snooping loose-state detect *number*

The default number of offline terminal probing times in ND Snooping loose mode is **12**.

1.8 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 [*mac-address*] [*ipv6-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]	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-type interface-number*]	Clears all packet statistics or packet statistics on an interface.
debug ipv6 nd snooping	Debugs ND Snooping events.

1.9 Configuration Examples

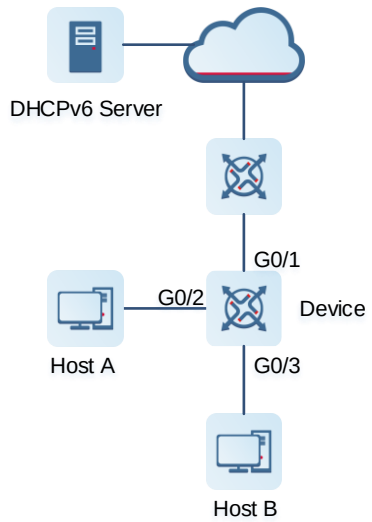
1.9.1 Configuring ND Guard

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. Verification

Display the ND Snooping binding entries detected on GigabitEthernet 0/1.

```
Device> enable
Device# show ipv6 nd snooping binding interface gigabitethernet 0/1
Total number of bindings: 5
VLAN MAC address     Interface    State        IPv6 address                    Life
time(s) -    b8ac.6fc8.8b9a   Gi0/1       VALID       2018:5::1
14376       -    b8ac.6fc8.8b9a   Gi0/1       VALID
2018:5::c58f:91d1:3dab:4e85       14381
-    b8ac.6fc8.8b9a   Gi0/1       VALID       fe80::c58f:91d1:3dab:4e85
14376
```

Display the ND Snooping binding entries detected on GigabitEthernet 0/2.

```
Device> enable
Device# show ipv6 nd snooping binding interface gigabitethernet 0/2
Total number of bindings: 5
VLAN MAC address     Interface    State        IPv6 address                    Life
time(s) -    b8ac.6fc8.8bca   Gi0/2       VALID       2008:5::1
13376       -    b8ac.6fc8.8bca   Gi0/2       VALID
2008:5::c58f:92d1:3dab:4e85       13381
-    b8ac.6fc8.8bca   Gi0/2       VALID       fe80::c58f:92d1:3dab:4e85
13376
```

6. 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 6
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 7
1.5.1 Overview 7
1.5.2 Restrictions and Guidelines 8
1.5.3 Procedure 8
1.6 Configuring the TCP Path MTU Discovery Function 8
1.6.1 Overview 8
1.6.2 Restrictions and Guidelines 8

1.6.3 Procedure....8
1.7 Configuring MSS for a TCP Connection....9
1.7.1 Overview....9
1.7.2 Restrictions and Guidelines....9
1.7.3 Procedure....9
1.8 Configuring TCP Connection Exception Detection....9
1.8.1 Overview....9
1.8.2 Procedure....10
1.9 Monitoring....10

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 RFC 793 of the Internet Engineering Task Force (IETF).

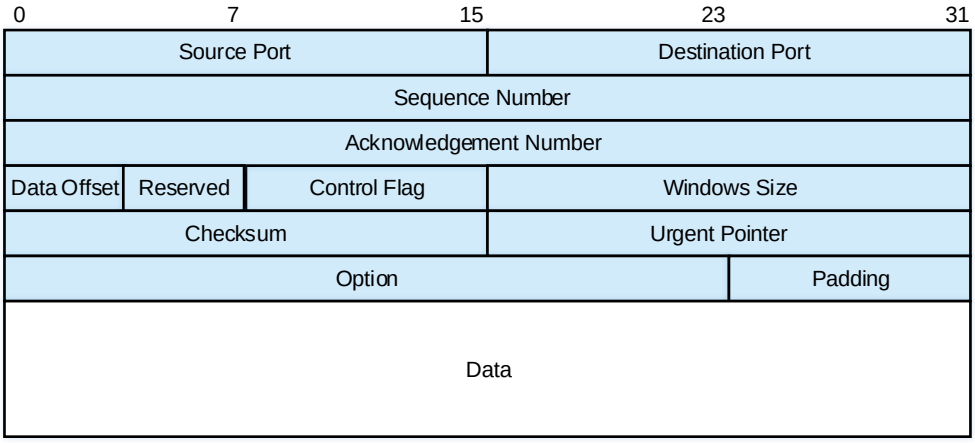
An interconnected network is very different from a single network in that topologies, bandwidth, latency, packet sizes, and other parameters may be entirely different in different parts of the interconnected network. TCP is designed to adapt dynamically to these features of interconnected networks and 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

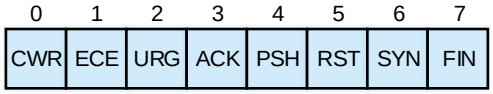


Field descriptions are as follows:

- **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



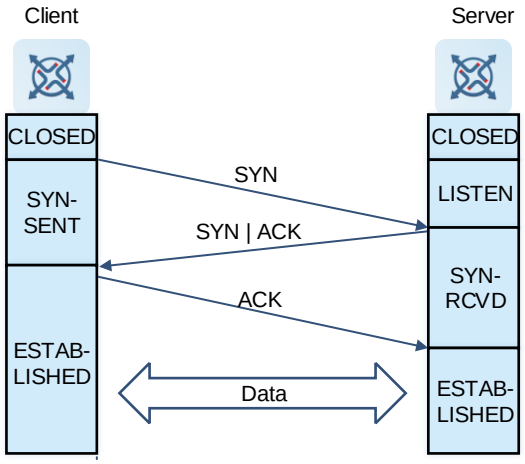
  - Congestion window reduced (**CWR**): The **CWR** flag and the **ECE** flag behind are used for the Explicit Congestion Notification (**ECN**) field in the IP header. When the **ECE** flag is **1**, the peer is notified to make the congestion window smaller.
  - ECN-Echo (**ECE**): The **ECE** flag 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 Reset packet with **RST** value of **1** 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 Reset packet with **RST** set to **1**, the connection is 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.

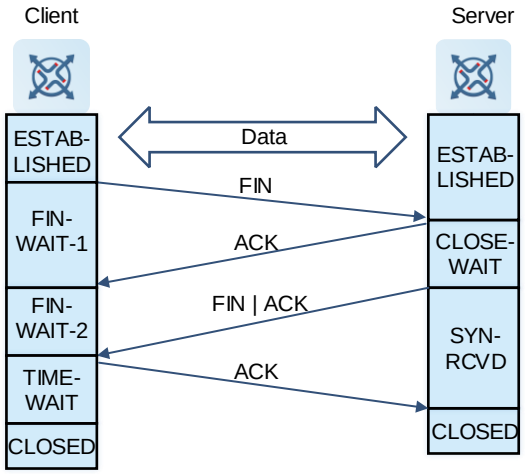
(5) The server receives the ACK packet from the client, confirming that the data transmission from the server to the client is normal. The server ends the SYN-SENT phase, and enters the ESTABLISHED phase.

(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 IPv4 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

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 RFC 1191 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 multiple 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 the TCP Path MTU Discovery Function
- 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.

- The IPv4 TCP and IPv6 TCP configuration commands are the same.

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.

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.

- The IPv4 TCP and IPv6 TCP configuration commands are the same.

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.

1.6 Configuring the TCP Path MTU Discovery Function

1.6.1 Overview

The path MTU discovery function of TCP is implemented according to RFC 1191 to improve the network bandwidth utilization. When TCP is applied to bulk transmit chunk data, this function can improve transmission performance greatly.

After discovering the path MTU, TCP can use a larger MSS to detect a new path MTU at intervals. When the device discovers a path MTU smaller than the MSS negotiated by both ends of a TCP connection, the device tries to discover a larger path MTU at intervals. The detection process is stopped when the path MTU reaches the MSS or the user turns off the timer.

1.6.2 Restrictions and Guidelines

Perform the configuration on both ends of a TCP connection.

- Run the **ip tcp path-mtu-discovery** command to enable the IPv4 Path MTU discovery function of TCP. Run the **no** form of this command to disable the function.
  - Run the **age-timer** *time* command to configure the interval for a new detection after TCP discovers the path MTU in minutes. The value range is from 10 to 30. The default value is 10.
  - Run the **age-timer infinite** command to stop detection after TCP discovers the path MTU.
- The IPv6 Path MTU discovery function of TCP is enabled permanently and cannot be disabled.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IPv4 Path MTU discovery function.

ip tcp path-mtu-discovery [**age-timer** *time* | **age-timer infinite**]

The IPv4 Path MTU discovery function of TCP is disabled by default.

1.7 Configuring MSS for a TCP Connection

1.7.1 Overview

TCP negotiates about the Maximum Segment Size (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.

1.7.2 Restrictions and Guidelines

- Perform the configuration on both ends of a TCP connection.
- The IPv4 TCP and IPv6 TCP configuration commands are the same.
- 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.

1.7.3 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*

Default MSS Upper Limit = MTU – Header Length – TCP Header Length

Note

Upper IPv4 TCP MSS Limit = IPv4 Path MTU – 20-Byte IPv4 Header –20-Byte TCP Header

Upper IPv6 TCP MSS Limit = IPv6 Path MTU – 20-Byte IPv4 Header –20-Byte TCP Header

1.8 Configuring TCP Connection Exception Detection

1.8.1 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.

The IPv4 TCP and IPv6 TCP configuration commands are the same.

1.8.2 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.

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 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** *ipv4-address*] [**local-port** *port-number*] [**peer-ip** *ipv4-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]	Displays the basic information about an IPv4 TCP connection.
show tcp connect statistics [**local-ip** *ipv4-address*] [**local-port** *port-number*] [**peer-ip** *ipv4-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]	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.
show ipv6 tcp connect [**local-ipv6** *ipv6-address*] [**local-port** *port-number*] [**peer-ipv6** *ipv6-address*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]	Displays the basic information about an IPv6 TCP connection.
show ipv6 tcp connect statistics [**local- ipv6** *ipv6*] [**local-port** *port-number*] [**peer- ipv6** *ipv6*] [**peer-port** *port-number*] [**vrf-name** *vrf-name*]	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*] [**vrf-name** *vrf-name*]	Displays the path MTU information of IPv6 TCP.
show ipv6 tcp port [*port-number*]	Displays the usage of IPv6 TCP port.
show tcpip { **capacity** | **client** [**service**] | **data-origin** | **database** { **arp** | **data-origin** | **nd** } | **direct-vlan** | **func-perf** | **interface** { *interface-type interface-number* [**extend**] | **extend** } | **ipv6-statistic** | **vrf-forward** [*interface-type interface-number*] } | **kernel-statistic** | **logging** { **error** | **freq-info** | **native-linux** | **startup** | **test** | **testv6** | **vrf** } | **lsm-statistic** | **memory** | **nsm-statistic** | **rdnd-statistic** | **ref-statistic** | **server-statistic** [*client-id*] | **sql** | **statistic** | **sync-client** | **sync-server-statistic** [*client-pid*] | **vrf** { **forward-version** [*vrf-name*] | **pseudo-instance** | **version** [*vrf-name*] } }	Displays information about the TCP/IP component.
debug ip tcp packet [**in** | **out**] [**local-ip** *ipv4-address*] [**peer-ip** *ipv4-address*] [**global** | **vrf** *vrf-name*] [**local-port** *port-number*] [**peer-port** *port-number*] [**deeply**]	Debugs IPv4 TCP packets.
debug ip tcp transactions [**local-ip** *ipv4-address*] [**peer-ip** *ipv4-address*] [**local-port** *port-number*] [**peer-port** *port-number*]	Debugs IPv4 TCP connections.
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 2
1.2 Configuration Task Summary 2
1.3 Configuring REF Load Balancing 3
1.3.1 Overview 3
1.3.2 Procedure 3
1.4 Configuring ECMP to Conduct Load Balancing According to a Fixed Profile 3
1.4.1 Overview 3
1.4.2 Restrictions and Guidelines 4
1.4.3 Procedure 4
1.5 Configuring Illegitimate Address Check 4
1.5.1 Overview 4
1.5.2 Restrictions and Guidelines 5
1.5.3 Procedure 5
1.6 Monitoring 5
1.7 Configuration Examples 7
1.7.1 Configuring a Load Balancing Policy 7

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.

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 Illegitimate Address Check

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 running the **ip ref load-balance** command, you can configure the following parameters to select the ECMP load balancing mode using a fixed profile.
  - **dst-ip**: Performs load balancing based on the destination IP addresses of packets.
  - **src-dst-ip-dst-l4port**: Performs load balancing based on the source IP addresses, destination IP addresses, 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 { **dst-ip** | **src-dst-ip** | **src-dst-ip-src-dst-l4port** | **src-ip** }

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.

(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.

(5) (Optional) Configure the ECMP hash algorithm mode.

ip ref algorithm mode *hash-number*

The default ECMP hash algorithm mode is 0.

1.5 Configuring Illegitimate Address Check

1.5.1 Overview

REF is capable of checking the destination IP addresses of IPv4 packets in a network, filtering out packets with illegitimate addresses, and recording these illegitimate addresses.

After the illegitimate address check function of REF is enabled, the device will check the destination IP addresses of IPv4 packets. The following types of addresses are considered illegitimate:

- Host addresses 0 (including 0.0.0.0).
- Loopback addresses (127.0.0.0–127.255.255.255).
- Class E addresses (240.0.0.0–255.255.255.254).

Invalid packets containing destination IP addresses that meet the above rules will be discarded by the device, and the illegitimate addresses will be logged.

1.5.2 Restrictions and Guidelines

REF can filter out class E addresses and loopback addresses and find out illegitimate addresses with the host address of 0 based on the specified mask length.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure illegitimate address check.

ip ref check [**masklen** *mask-length*]

IPv4 REF does not check illegitimate destination IP addresses 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 efmp counter	Displays the number of REF packets of different services.
show efmp diagnosis { **drop** [**slot** *slot-id*] | **statistics** [**details**] [**slot** *slot-id*] }	Displays packet diagnostics information.
clear efmp diagnosis { **drop** | **statistics** }	Clears packet diagnostics information.
show ip logging [**clear**]	Displays the recorded illegitimate addresses.
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** | *ipv4-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.
show ip ref resolve-list	Displays the next hop resolved by IPv4 REF.
show ip ref exact-route [**vrf** *vrf-name*] *source-ipv4-address destination-ipv4-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 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*] | [**device** *device-id*] [**slot** *slot-id*]]	Displays the detailed routing information about an IPv4 route prefix or about all IPv4 route prefixes of the card in a specified slot.
show ip ref load-balance	Displays the configuration of the ECMP load balancing using a fixed 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 the actual 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*]	[**device** *device-id*] [**slot** *slot-id*]]	Displays the detailed routing information about an IPv6 route prefix or about all IPv6 route prefixes of the card in a specified slot.
ipv6 ref synchronize all	Synchronizes IPv6 routes between the hardware and software REF.

1.7 Configuration Examples

1.7.1 Configuring a Load Balancing Policy

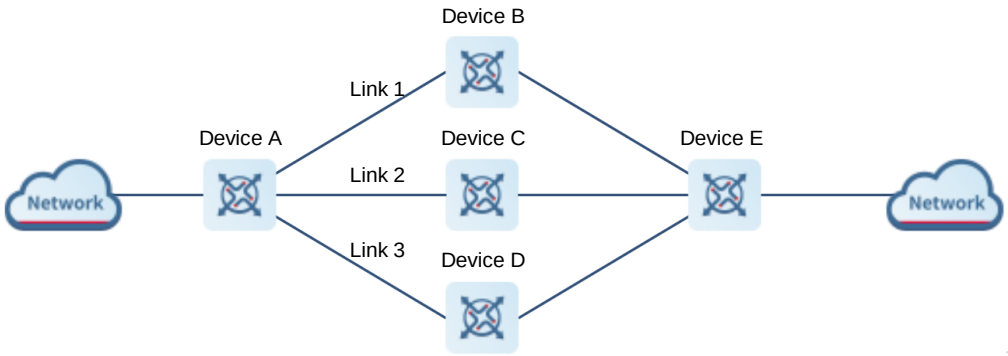
1. Requirements

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 a 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.

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
DeviceA(config)# ip ref algorithm mode 8
```

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.
Algorithm mode
  current: 8,  default: 0
```

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip ref algorithm mode 8
ip ref load-balance src-ip
ip ref hash-elasticity enable
```

IP Routing Configuration

1. Configuring IP Routing Basics
2. Configuring Static Routing
3. Configuring RIP
4. Configuring RIPng
5. Configuring OSPFv2
6. Configuring OSPFv3
7. Configuring VRF
8. Configuring Routing Policies
9. Configuring PBR
10. Configuring Routing Keys

Contents

1 Configuring IP Routing Basics 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

1.4.5 Preventing a Route from Being Iterated to a Black-Hole Route 7

1.4.6 Preventing a Route from Being Iterated to a Default Route 7

1.5 Configuring ARP-to-Route 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-Route Conversion 8
1.5.5 Enabling Delayed Redistribution for ARP-to-Route Conversion 8
1.5.6 Configuring the Tag Attribute for ARP-to-Route Conversion 8
1.5.7 Enabling Proxy ARP 9
1.6 Configuring ND-to-Route Conversion 9
1.6.1 Overview 9
1.6.2 Restrictions and Guidelines 9
1.6.3 Configuration Tasks 9
1.6.4 Configuring the Interface to Enable ND Conversion to Route 10
1.6.5 Configuring Delayed Redistribution of ND-to-Route 11
1.6.6 Configuring Tag Attribute of ND-to-Route Conversion 11
1.6.7 Configuring to Ignore Warning Log of ND Conversion to Route 12
1.6.8 Configuring ND Proxy 12
1.7 Monitoring 13

1 Configuring IP Routing Basics

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.

  The routing function is IPv4 routing function. 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-route conversion

  Enable ARP-to-route 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
- Preventing a Route from Being Iterated to a Black-Hole Route
- Preventing a Route from Being Iterated to a Default Route

(3) (Optional) Configuring ARP-to-Route Conversion

a Configuring the Interface to Enable ARP-to-Route Conversion

b (Optional) Enabling Delayed Redistribution for ARP-to-Route

c (Optional) Configuring the Tag Attribute for ARP-to-Route Conversion

d (Optional) Enabling Proxy ARP

(4) (Optional) Configuring ND-to-Route Conversion

a Configuring the Interface to Enable ND Conversion to Route

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

e (Optional) Configuring ND Proxy

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 number of equal-cost routes is 8 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
- **Preventing a Route from Being Iterated to a Default Route**
- **Preventing a Route from Being Iterated to a Black-Hole Route**

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.

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

1.4.5 Preventing a Route from Being Iterated to a Black-Hole Route

1. Overview

This function allows a device to divert all traffic to the standby path when the active path fails, so as to avoid the loss of traffic caused by the import of a black-hole route.

2. Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Configure preventing a route from being iterated to a black-hole route.
ip recur-route over blackhole-route disable

By default, a route is allowed to be iterated to a black-hole route.

1.4.6 Preventing a Route from Being Iterated to a Default Route

3. Overview

When you do not want to select the default route for transmitting traffic, you can use this function to configure the device to not select the default route egress during recursive routing.

4. Restrictions and Guidelines

- This command must be configured when the default route egress is not the expected service egress.

5. Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Configure preventing a route from being iterated to a default route.
ip recur-route over default-route disable

By default, a route is allowed to be iterated to a default route.

1.5 Configuring ARP-to-Route 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-route conversion configuration includes the following tasks:

(1) Configuring the Interface to Enable ARP-to-Route Conversion

(2) (Optional) Enabling Delayed Redistribution for ARP-to-Route

(3) (Optional) Configuring the Tag Attribute for ARP-to-Route Conversion

(4) (Optional) Enabling Proxy ARP

1.5.4 Configuring the Interface to Enable ARP-to-Route 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-route conversion on a specified interface.

ip route arp-to-host interface *interface-type interface-number*

The ARP-to-route conversion function is disabled on an interface by default.

1.5.5 Enabling Delayed Redistribution for ARP-to-Route Conversion

1. Overview

To prevent route flapping caused by ARP entry changes, ARP entries can be converted into routes with a delay.

2. Restrictions and Guidelines

After delayed redistribution is configured, ARP validation messages are redistributed after the specified delay. This function does not take effect on ARP invalidation messages for withdrawing routes, and such messages are redistributed immediately.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable delayed redistribution for ARP-to-route conversion.

ip route arp-to-host delay-time *time-number*

Delayed redistribution for ARP-to-route conversion is disabled by default.

1.5.6 Configuring the Tag Attribute for ARP-to-Route Conversion

1. Overview

Set the tag attribute for ARP-to-route conversion to facilitate 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 for ARP-to-route conversion.

ip route arp-to-host tag *tag-number*

No tag attribute is configured for ARP-to-route conversion by default.

1.5.7 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 SVI configuration mode.

interface *vlan interface-number*

(4) Enable the proxy ARP.

local-proxy-arp

The local proxy ARP function is disabled by default on the SVI interface.

1.6 Configuring ND-to-Route Conversion

1.6.1 Overview

Similar to ARP-to-route 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

(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

(5) (Optional) Configuring ND Proxy

1.6.4 Configuring the Interface to Enable ND Conversion to Route

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** *ipv6-prefix/prefix-length*] [**prefix-len** *mask-length*]

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

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 configuration 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.

1.7 Monitoring

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

Run the **debug** command to 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 [[*ipv4-address* [*mask* [**longer-prefixes**]] | **aggregate** | **arphost** | **bgp** | **connected** | **count** | **database** [*ipv4-address/mask-length*] | [**detail** | **ecmp** | **fast-reroute** | **normal**] [*ipv4-address* [*mask*]] | **isis** [*tag*] | **ospf** [*process-id*] | **rip** | **static** [**web**] | **weight** | **tag**]	Displays the IPv4 routing table.
show ipv6 route [**vrf** *vrf-name*] [**bgp** | **connected** | **database** [*ipv6-prefix/prefix-length*] | [**fast-reroute**] *ipv6-prefix/prefix-length* [**longer-prefixes**] | **isis** | **local** | **ndroute** | **ospf** | **rip** | **static** [**web**] | **tag** | **weight**]	Displays the IPv6 routing table.
show ip route [**vrf** *vrf-name*] **recursive** *ipv4-address/mask*	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.

Command	Purpose
show ipv6 route [**vrf** *vrf-name*] **summary**	Displays the statistics of all the IPv6 routing tables.
show nsm develop { **basic** | **bfd neighbor** | **block** | **client** [*client-name*] | **interface** [*interface-type interface-number*] | **memory** | **mom** | **route-num** | **vrf** [*vrf-name*] }	Displays information about routes.
show route-res usage [**all** | **slot** *slot-id* | **switch** *switch-id* **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.
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 Routing 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 4

1.3.4 Configuring a Static IPv4 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 Default IPv4 Gateway on a Layer-3 Device 6

1.4.6 Configuring the Default IPv6 Gateway on a Layer-3 Device 6

1.4.7 Configuring the Default IPv4 Network on a Layer-3 Device 7

1.5 Configuring Routing Black Hole 7

1.5.1 Overview 7

1.5.2 Procedure 8

1.6 Configuring Route Limitations 8
1.6.1 Overview 8
1.6.2 Configuration Tasks 8
1.6.3 Configuring the Maximum Number of IPv4 Static Routes 8
1.6.4 Configuring the Maximum Number of IPv6 Static Routes 9
1.6.5 Prohibiting Static Routing Across VRFs 9
1.6.6 Configuring the Maximum Number of VRF Routes 9
1.7 Correlating a Static Route with BFD 10
1.7.1 Overview 10
1.7.2 Restrictions and Guidelines 10
1.7.3 Configuration Tasks 10
1.7.4 Configuring Correlation of IPv4 Static Routes with BFD 10
1.7.5 Configuring Correlation of IPv6 Static Routes with BFD 10
1.8 Configuring Static Fast Reroute 11
1.8.1 Overview 11
1.8.2 Restrictions and Guidelines 11
1.8.3 Procedure 11
1.9 Configuring Correlation of Static Routes with ARP 12
1.9.1 Overview 12
1.9.2 Procedure 12
1.10 Monitoring 12
1.11 Configuration Examples 13
1.11.1 Configuring an IPv4 Static Route 13
1.11.2 Configuring Correlation of IPv4 Static Routes with Track 17

1.11.3 Configuring Correlation of Static Routes with BFD.....20

1.11.4 Configuring Fast Reroute.....22

1 Configuring Static Routing

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

  On a Layer-3 device which used the **no ip routing** command, run the **ip default gateway** command to generate a default route.

On a Layer-3 device which used the **no ipv6 unicast routing** command, run the **ipv6 default gateway** command to generate a default route.

- Static default route

  On a Layer-3 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 a Static IPv4 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 Default IPv4 Gateway on a Layer-3 Device
- Configuring the Default IPv6 Gateway on a Layer-3 Device
- Configuring the Default IPv4 Network on a Layer-3 Device

(3) (Optional) Configuring Routing Black Hole Black Hole The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

(4) (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

(5) (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

(6) (Optional) Configuring Static Fast Reroute

(7) (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 on a Layer-3 device, 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 on a Layer-3 device, 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 a Static IPv4 Route
- Configuring an IPv6 Static Route

1.3.4 Configuring a Static IPv4 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* | *mask-length* } { *ipv4-address* [**global**] | *interface-type interface-number* [*ipv4-address* [**arp** | **global**] *] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | **tag** *tag* | [**track** *object-number*] [**permanent**] | **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-type interface-number* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance* | **description** *description-text* | **tag** *tag* | **weight** *number*] *

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 Default IPv4 Gateway on a Layer-3 Device
- Configuring the Default IPv6 Gateway on a Layer-3 Device
- Configuring the Default IPv4 Network on a Layer-3 Device

1.4.3 Configuring the IPv4 Gateway

1. Overview

On a Layer-3 device which used the **no ip routing** command, 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 Layer-2 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 default gateway is configured by default.

1.4.4 Configuring the IPv6 Gateway

1. Overview

On a Layer-3 device which used the **no ipv6 unicast routing** command, 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 Layer-2 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 default IPv6 gateway is configured by default.

1.4.5 Configuring the Default IPv4 Gateway on a Layer-3 Device

1. Overview

On a Layer-3 switching device and routing 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 default IPv4 gateway on a Layer-3 device.

ip route [**vrf** *vrf-name*] **0.0.0.0 0.0.0.0** { *ipv4-address* [**global** | **nexthop-vrf** *vrf-name1*] | *interface-type interface-number* [*ipv4-address* [**arp** [**global**] | **global** [**arp**] | **nexthop-vrf** *vrf-name1* [**arp**]]] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | **tag** *tag* | [**track** *object-number*] [**permanent**] | **weight** *number*] *

ip route 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**]

No default IPv4 gateway is configured on the Layer-3 device.

1.4.6 Configuring the Default IPv6 Gateway on a Layer-3 Device

1. Overview

On a Layer-3 switching 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 default IPv6 gateway on a Layer-3 device.

ipv6 route [**vrf** *vrf-name*] **::/0** { *ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }] | *interface-type interface-number* [*ipv6-address* [**nexthop-vrf** { *vrf-name1* | **default** }]] } [*distance* | **description** *description-text* | **tag** *tag* | **weight** *number*] *

No default IPv6 gateway is configured on the Layer-3 device.

1.4.7 Configuring the Default IPv4 Network on a Layer-3 Device

1. Overview

On a Layer-3 switching device, when the routing for packet sending cannot match an accurate route, the default network 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 default IPv4 network on a Layer-3 device.

ip default-network *network*

No default IPv4 network is configured on the Layer-3 device.

1.5 Configuring Routing Black Hole

1.5.1 Overview

Routing black hole can avoid the problem of route loop when the route summary and default route are configured at the same time. If the 192.168.1.0/24 and 192.168.2.0/24 network segments exist on the internal network, the default route of Router A will point to the gateway, and the two internal network segments are summarized into 192.168.0.0/16 and notified to the gateway through the dynamic routing protocol. When the gateway initiates access to the address 192.168.3.1/24 not existing on the internal network to Router A, Router A will forward the access request back to the gateway according to the default route, thus causing a route loop. Null 0 is a virtual interface never in Down status, and Router A is configured with 192.168.0.0/16 to point to Null 0. Then, the request sent by the gateway to the router destination address 192.168.3.1/24 will be discarded by Router A.

Configuring a routing black hole can make full use of the forwarding performance of routers and avoid route loops.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an aggregated route.

ip route aggregate [**vrf** *vrf-name*] *network mask* **Null 0** [**tag** *tag*]

The aggregated route is disabled by default.

1.6 Configuring Route Limitations

1.6.1 Overview

This function limits the number of equal-cost routes and number of static routes, or disables routing.

1.6.2 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

1.6.3 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 { *route-limit* | **default-vrf** *default-vrf-route-limit* | **vrf** *vrf-name vrf-route-limit* }

The configured maximum number of static routes is 1000 by default.

1.6.4 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 { *route-limit* | **default-vrf** *default-vrf-route-limit* | **vrf** *vrf-name vrf-route-limit* }

The configured maximum number of static routes is 1000 by default.

1.6.5 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.

1.6.6 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.

1.7 Correlating a Static Route with BFD

1.7.1 Overview

A static route can quickly detect a route failure with the help of BFD.

1.7.2 Restrictions and Guidelines

- You must configure a static route before configuring this function.
- Before configuring this function, you must configure BFD session parameters using the **bfd interval** command.

1.7.3 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

1.7.4 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.

1.7.5 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.

1.8 Configuring Static Fast Reroute

1.8.1 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.

1.8.2 Restrictions and Guidelines

- You must configure a static route before configuring this function.
- You must configure a route map before configuring this function.

1.8.3 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.

ipv6 fast-reroute [**vrf** *vrf-name*] **static route-map** *route-map-name*

The IPv6 static fast reroute function is disabled by default.

1.9 Configuring Correlation of Static Routes with ARP

1.9.1 Overview

This function is used to configure correlation of static routes with ARP so that ARP requests are actively sent when ARP fails.

1.9.2 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.

1.10 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.

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
clear ip route arp scan times	Clears the ARP request transmission count and starts counting again.
show ip redirects	Displays the default gateway.

Command	Purpose
show ipv6 redirects	Displays the default IPv6 gateway.

1.11 Configuration Examples

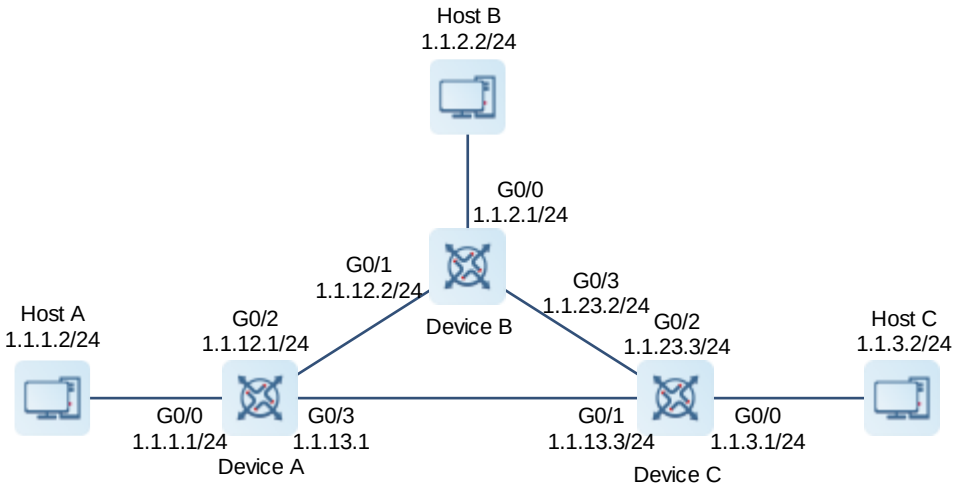
1.11.1 Configuring an IPv4 Static Route

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/0
DeviceA(config-if-GigabitEthernet 0/0)# no switchport
DeviceA(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/0)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# no switchport
```

```
DeviceA(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0
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)# ip address 1.1.13.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/3)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/0
DeviceB(config-if-GigabitEthernet 0/0)# no switchport
DeviceB(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/0)# exit
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# no switchport
DeviceB(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitethernet 0/3
DeviceB(config-if-GigabitEthernet 0/3)# no switchport
DeviceB(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/3)# exit
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface gigabitethernet 0/0
DeviceC(config-if-GigabitEthernet 0/0)# no switchport
DeviceC(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/0)# exit
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# no switchport
DeviceC(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/1)# exit
DeviceC(config)# interface gigabitethernet 0/2
DeviceC(config-if-GigabitEthernet 0/2)# no switchport
DeviceC(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/2)# exit
```

(2) Enable the IPv4 static route function.

Configure Device A.

```
DeviceA(config)# ip route 1.1.2.0 255.255.255.0 gigabitethernet 0/2 1.1.12.2
DeviceA(config)# ip route 1.1.3.0 255.255.255.0 gigabitethernet 0/3 1.1.13.3
```

Configure Device B.

```
DeviceB(config)# ip route 1.1.1.0 255.255.255.0 gigabitethernet 0/1 1.1.12.1
DeviceB(config)# ip route 1.1.3.0 255.255.255.0 gigabitethernet 0/3 1.1.23.3
```

Configure Device C.

```
DeviceC(config)# ip route 1.1.2.0 255.255.255.0 gigabitethernet 0/2 1.1.23.2
DeviceC(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.

```
DeviceA# 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    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 0/3
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.

```
DeviceB# 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
S    1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/1
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.

```
DeviceC# 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
S    1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/1
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
 no switchport
 ip address 1.1.1.1 255.255.255.0
!
interface gigabitethernet 0/2
 no switchport
 ip address 1.1.12.1 255.255.255.0
!
interface gigabitethernet 0/3
 no switchport
 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
 no switchport
 ip address 1.1.2.1 255.255.255.0
!
```

```
interface gigabitethernet 0/1
 no switchport
 ip address 1.1.12.2 255.255.255.0
!
interface gigabitethernet 0/3
 no switchport
 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
 no switchport
 ip address 1.1.3.1 255.255.255.0
!
interface gigabitethernet 0/1
 no switchport
 ip address 1.1.13.3 255.255.255.0
!
interface gigabitethernet 0/2
 no switchport
 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.

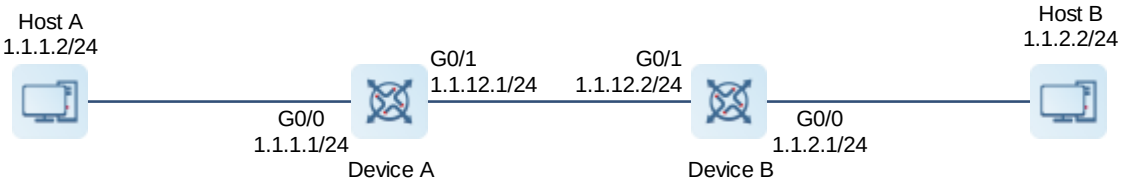
1.11.2 Configuring Correlation of IPv4 Static Routes with Track

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/0
DeviceA(config-if-GigabitEthernet 0/0)# no switchport
DeviceA(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/0)# exit
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/0
DeviceB(config-if-GigabitEthernet 0/0)# no switchport
DeviceB(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/0)# exit
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# no switchport
DeviceB(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure the track function.

Configure Device A.

```
DeviceA(config)# track 2 interface gigabitethernet 0/1 line-protocol
DeviceA(config-track)# exit
```

Configure Device B.

```
DeviceB(config)# track 2 interface gigabitethernet 0/1 line-protocol
DeviceB(config-track)# exit
```

(3) Configure correlation of static routes with track.

Configure Device A.

```
DeviceA(config)# ip route 1.1.2.0 255.255.255.0 gigabitethernet 0/1 1.1.12.2 track
2
```

Configure Device B.

```
DeviceB(config)# ip route 1.1.1.0 255.255.255.0 gigabitethernet 0/1 1.1.12.1 track
2
```

5. Verification

Display the statistics of Track 2.

```
DeviceA# 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.

```
DeviceA# show ip route track-table
ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.2 track 2 up
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/0
 no switchport
 ip address 1.1.1.1 255.255.255.0
!
interface gigabitethernet 0/1
 ip address 1.1.12.1 255.255.255.0
!
track 2 interface gigabitEthernet 0/1 line-protocol
!
ip route 1.1.2.0 255.255.255.0 gigabitEthernet 0/1 1.1.12.2 track 2
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/0
 no switchport
```

```
 ip address 1.1.2.1 255.255.255.0
!
interface gigabitethernet 0/1
 ip address 1.1.12.2 255.255.255.0
!
track 2 interface gigabitethernet 0/1 line-protocol
!
ip route 1.1.1.0 255.255.255.0 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.

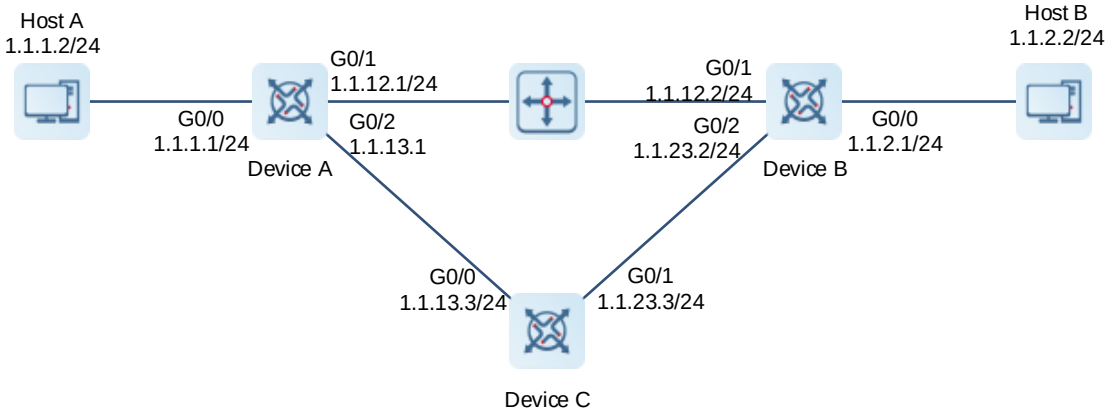
1.11.3 Configuring Correlation of Static Routes with BFD

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip route 1.1.2.0 255.255.255.0 gigabitEthernet 0/1 1.1.12.2
DeviceA(config)# ip route 1.1.2.0 255.255.255.0 gigabitEthernet 0/2 1.1.13.3 40
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip route 1.1.1.0 255.255.255.0 gigabitEthernet 0/1 1.1.12.1
DeviceB(config)# ip route 1.1.1.0 255.255.255.0 gigabitEthernet 0/2 1.1.23.3 40
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ip route 1.1.1.0 255.255.255.0 gigabitethernet 0/0 1.1.13.1
DeviceC(config)# ip route 1.1.2.0 255.255.255.0 gigabitethernet 0/1 1.1.23.2
```

(3) Configure BFD for an interface.

Configure Device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# bfd interval 100 min_rx 100 multiplier 3
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure Device B.

```
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# bfd interval 100 min_rx 100 multiplier 3
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

(4) Configure correlation of static routes with BFD.

Configure Device A.

```
DeviceA(config)# ip route static bfd gigabitethernet 0/1 1.1.12.2
```

Configure Device B.

```
DeviceB(config)# ip route static bfd gigabitethernet 0/1 1.1.12.1
```

5. Verification

Display the states of BFD neighbors.

```
DeviceA# 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.

```
DeviceA# 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 100 min_rx 100 multiplier 3
!
ip route 1.1.2.0 255.255.255.0 gigabitEthernet 0/1 1.1.12.2
ip route 1.1.2.0 255.255.255.0 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 100 min_rx 100 multiplier 3
!
ip route 1.1.1.0 255.255.255.0 gigabitethernet 0/1 1.1.12.1
ip route 1.1.1.0 255.255.255.0 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 1.1.1.0 255.255.255.0 gigabitethernet 0/0 1.1.13.1
ip route 1.1.2.0 255.255.255.0 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.

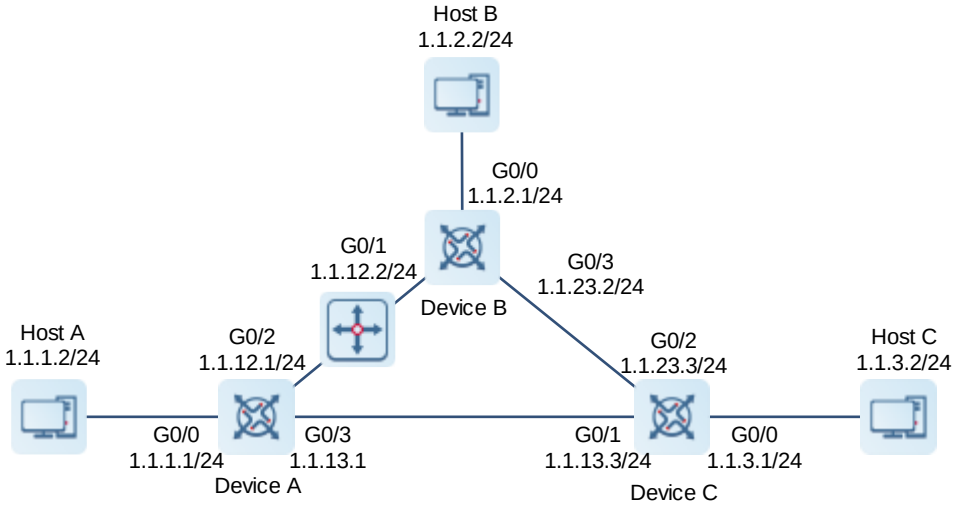
1.11.4 Configuring Fast Reroute

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# route-map fast-reroute
DeviceA(config-route-map)# set fast-reroute backup-interface gigabitethernet 0/2
backup-nexthop 1.1.12.2
```

(4) Configure static fast reroute.

```
DeviceA(config-route-map)# exit
DeviceA(config)# ip fast-reroute static route-map fast-reroute
```

5. Verification

Display the primary and backup routes on Device A.

```
DeviceA# show ip route fast-reroute
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       LA - Local aggregate route
       * - 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 10
1.3.4 Enabling RIP Process 11
1.3.5 Configuring Association Between RIP Instances and VRF 11
1.3.6 Configuring Association with the Local Network 12
1.3.7 Configuring RIP Version 12
1.3.8 Configuring Split Horizon 13
1.3.9 Configuring a Passive Interface 14
1.3.10 Enabling Triggered Updates 14
1.4 Enabling RIP Route Summarization 15
1.4.1 Overview 15
1.4.2 Restrictions and Guidelines 15
1.4.3 Configuration Tasks 15

1.4.4 Configuring to Enable Automatic Route Summarization Function 16
1.4.5 Configuring RIP Route Summarization on an Interface 16
1.5 Configuring RIP Route Filtering Rules 17
1.5.1 Overview 17
1.5.2 Restrictions and Guidelines 17
1.5.3 Configuration Tasks 17
1.5.4 Configuring to Filter the Received RIP Routing Information 17
1.5.5 Configuring to Filter the Sent RIP Routing Information 18
1.6 Configuring to Adjust RIP Routing 19
1.6.1 Overview 19
1.6.2 Restrictions and Guidelines 19
1.6.3 Configuration Tasks 19
1.6.4 Configuring to Modify the Management Distance of a RIP Route 19
1.6.5 Configuring to Increase the Metric of a Received or Sent RIP Route 20
1.6.6 Configuring the Default Metric of an External Route Redistributed to RIP 20
1.7 Modifying Timers 21
1.7.1 Overview 21
1.7.2 Restrictions and Guidelines 21
1.7.3 Configuration Tasks 21
1.7.4 Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route 21
1.7.5 Configuring the Sending Delay Between RIP Route Update Packets 22
1.8 Configuring RIP Route Distribution 23

1.8.1 Overview 23
1.8.2 Restrictions and Guidelines 23
1.8.3 Configuration Tasks 23
1.8.4 Configuring to Advertise a Default Route to Neighbors 23
1.8.5 Configuring to Advertise a Default Route to Neighbors on an Interface 24
1.8.6 Configuring Route Redistribution 24
1.9 Controlling Interaction of RIP Packets 25
1.9.1 Overview 25
1.9.2 Restrictions and Guidelines 26
1.9.3 Configuration Tasks 26
1.9.4 Configuring to Send Unicast RIP Route Update Packets 26
1.9.5 Configuring to Send Broadcast RIPv2 Packets on an Interface 27
1.9.6 Configuring to Allow an Interface to Receive RIP Packets 28
1.9.7 Configuring to Allow an Interface to Send RIP Packets 28
1.9.8 Configuring to Allow an Interface to Send RIP Packets of a Specified Version 29
1.9.9 Configuring to Allow an Interface to Receive RIP Packets of a Specified Version 30
1.10 Configuring to Enable RIPv2 Authentication 31
1.10.1 Overview 31
1.10.2 Restrictions and Guidelines 31
1.10.3 Configuration Tasks 31
1.10.4 Configuring RIP Authentication Mode 31
1.10.5 Configuring a Key Chain for Authentication 32
1.10.6 Configuring a Key Chain for RIP Plain Text Authentication 33

1.11 Configuring BFD Correlation with RIP 34
1.11.1 Overview 34
1.11.2 Restrictions and Guidelines 34
1.11.3 Configuration Tasks 34
1.11.4 Configuring BFD Correlation with RIP Globally 34
1.11.5 Configuring BFD Correlation with RIP on an Interface 35
1.12 Configuring to Enable RIP Fast Reroute 36
1.12.1 Overview 36
1.12.2 Restrictions and Guidelines 36
1.12.3 Procedure 36
1.13 Enabling GR 37
1.13.1 Overview 37
1.13.2 Restrictions and Guidelines 37
1.13.3 Procedure 37
1.14 Configuring to Enable RIP Supernetting Routes 37
1.14.1 Overview 37
1.14.2 Restrictions and Guidelines 37
1.14.3 Procedure 38
1.15 Configuring MIB Binding 38
1.15.1 Overview 38
1.15.2 Restrictions and Guidelines 38
1.16 Configuring a Super VLAN to Enable RIP 39
1.16.1 Overview 39

1.16.2 Restrictions and Guidelines 39
1.16.3 Procedure 39
1.17 Enabling Source Address Verification 40
1.17.1 Overview 40
1.17.2 Restrictions and Guidelines 40
1.17.3 Procedure 40
1.18 Enabling Backup Route 40
1.1.2 Overview 40
1.1.3 Restrictions and Guidelines 40
1.1.4 Procedure 41
1.19 Monitoring 41
1.20 Configuration Examples 42
1.20.1 Building a RIP Routing Domain 42
1.20.2 Configuring RIP to Prevent Route Loop 47
1.20.3 Configuring External Routes Imported by RIP 50
1.20.4 Configuring Increasing the Metric of a RIP Interface 51
1.20.5 Configuring RIP to Distribute a Summarized Route 53

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 to120s. 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.

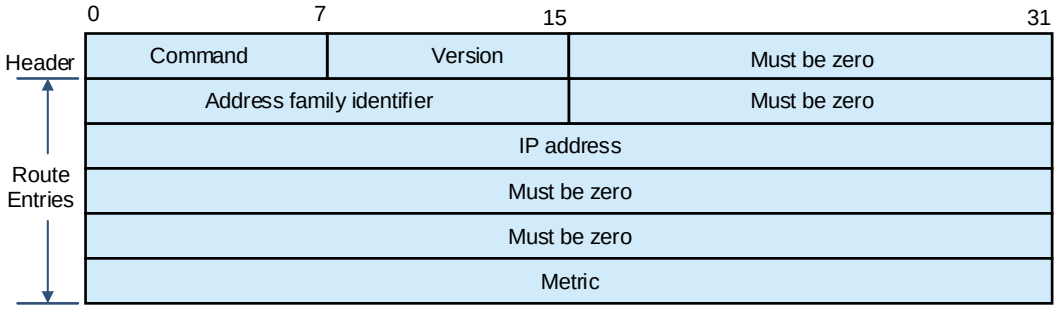
2. RIPv1 and RIPv2

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.

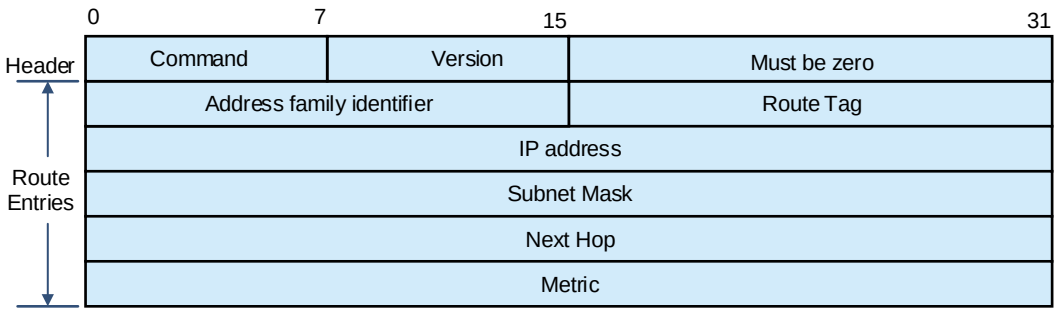
Figure 1-1 RIPv1 Packet Format



- 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.

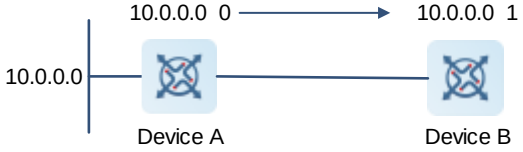
- Distance-vector algorithm

  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

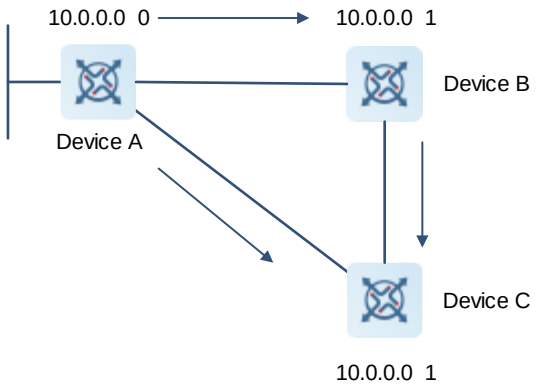


- Selecting the optimum route

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

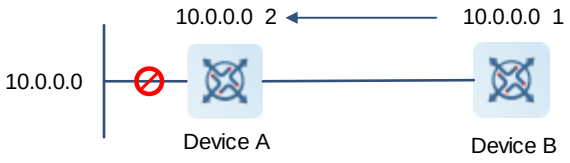
RIP uses functions such as split horizon and poison reverse to avoid route loops.

- 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



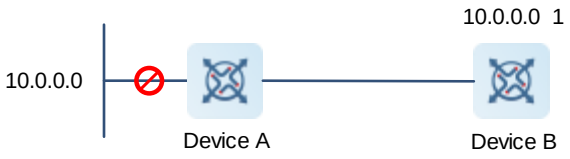
- Split horizon

  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



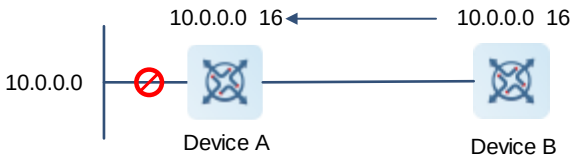
- Poison reverse

  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

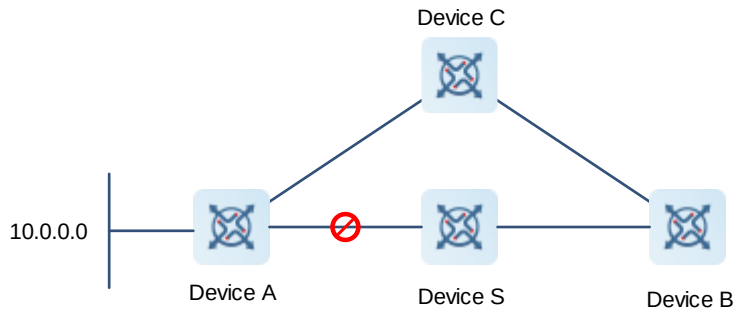
RIP uses the following functions to enhance protocol reliability.

- Correlate with BFD and 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 (Optional)Configuring Association Between RIP Instances and VRF

c (Optional)Configuring Association with the Local Network

d (Optional) Configuring RIP Version

e (Optional) Configuring Split Horizon

f (Optional) Configuring a Passive Interface

g (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.

a Configuring to Filter the Received RIP Routing Information

b 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.

a Configuring to Modify the Management Distance of a RIP Route

b Configuring to Increase the Metric of a Received or Sent RIP Route Metric

c 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.

a Configuring to Modify the Update Timer, Invalid Timer, Flush Timer, and Holddown Timer of a RIP Route

b 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.

a Configuring to Advertise a Default Route to Neighbors

b Configuring to Advertise a Default Route to Neighbors on an Interface

c Configuring Route Redistribution

(7) (Optional) Controlling Interaction of RIP Packets The following configuration tasks are optional. Select tasks for configuration according to actual condition.

a Configuring to Send Unicast RIP Route Update Packets

b Configuring to Send Broadcast RIPv2 Packets on an Interface

c Configuring to Allow an Interface to Receive RIP Packets

d Configuring to Allow an Interface to Send RIP Packets

e Configuring to Allow an Interface to Send RIP Packets of a Specified Version

f 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

a Configuring BFD Correlation with RIP Globally

b 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 MIB Binding

(14) (Optional) Configuring a Super VLAN to Enable RIP

(15) (Optional) Enabling Source Address Verification

(16) (Optional) Enabling Backup Route

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) (Optional)Configuring Association Between RIP Instances and VRF

(3) (Optional) Configuring Association with the Local Network

(4) (Optional) Configuring RIP Version

(5) (Optional) Configuring Split Horizon

(6) (Optional) Configuring a Passive Interface

(7) (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 Between RIP Instances and VRF

1. Overview

This command is used to create RIP instances to be associated with VRF, and enter the RIP IPv4 VRF address family configuration mode.

2. Restrictions and Guidelines

This function must be configured if you need to configure multiple RIP instances and associate them with VRF.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing configuration mode.

router rip

(4) Create RIP instances to be associated with VRF, and enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

By default, the address family of RIP protocol is disabled.

(5) Exit the RIP IPv4 VRF address family configuration mode.
exit-address-family

1.3.6 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) Configure association with the local network.

network *network-number* [*wildcard*]

1.3.7 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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.

1.3.8 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.

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI configuration mode.
  interface vlan *interface-number*
- Enter the loopback interface configuration mode.
  interface loopback *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.

1.3.9 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 route 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) Configure passive interfaces.

passive-interface { **default** | *interface-type interface-number* }

The passive interface function is disabled by default.

1.3.10 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 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.

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI configuration mode.
  interface vlan *interface-number*
- Enter the loopback interface configuration mode.
  interface loopback *interface-number*

(4) Enable triggered updates.

ip rip triggered [**retransmit-count** *count* | **retransmit-timer** *timer*]

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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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.

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI configuration mode.
  interface vlan *interface-number*
- Enter the loopback interface configuration mode.
  interface loopback *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 configuration mode.

router rip

(5) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(6) Filter the received RIP routing information.

distribute-list { *acl-name* | *acl-number* | **gateway** *prefix-list-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) 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 configuration mode.

router rip

(5) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(6) Filter the sent RIP routing information.

distribute-list { *acl-name* | *acl-number* | **prefix** *prefix-list-name* } **out** [*interface-type interface-number* | **connected** | **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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) Configure to increase the metric of a received or sent RIP route.

offset-list { *acl-name* | *acl-number* } { **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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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 RIP routing configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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

To enable the RIP routing domain to communicate with other ASs, you can inject a default route to other ASs into the RIP routing domain, or redistribute the routes of other ASs to RIP.

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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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.

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*
- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*
- Enter the SVI configuration mode.
  interface vlan *interface-number*
- Enter the loopback interface configuration mode.
  interface loopback *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 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) Redistribute routes and advertise external routes to neighbors.

redistribute { **connected** | **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.

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 RIP route 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Enable the RIP authentication mode.

ip rip authentication mode { **md5 | text** }

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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>

No interface-based matching rule is configured by default.

(5) Return to the global configuration mode.

exit

(6) Enter the RIP routing configuration mode.

router rip

(7) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(8) 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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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 MIB Binding

1.15.1 Overview

Since RIP MIB does not have RIP instances, you can only operate on the unique instance when operating RIP instances through SNMP. With this function, you can bind the MIB to the RIP instance of the specified VRF, and operate the RIP instance of the specified VRF through the SNMP protocol.

1.15.2 Restrictions and Guidelines

The RIP basic functions (with VRF parameters) must be configured.

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIP routing configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) Configure binding the MIB of RIP to the specified VRF instance.

enable mib-binding

By default, the MIB is bound to 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) Enter the SVI interface configuration mode.

interface vlan *interface-number*

(4) Enable RIP on a Super VLAN.

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 configuration mode.

router rip

(4) (Optional) Enter the RIP IPv4 VRF address family configuration mode.

address-family ipv4 vrf *vrf-name*

(5) Enables source address verification.

validate-update-source

The source address validation function for update packets is enabled by default.

1.18 Enabling Backup Route

1.1.2 Overview

After the backup route is enabled, the RIP database stores all RIP routes advertised by neighbors. In a non-ring topology, if the primary path in a multi-host route goes down, traffic is quickly and imperceptibly switched to a new path, avoiding the short-term interruption caused by route relearning.

1.1.3 Restrictions and Guidelines

- The basic RIP function must be configured.

- It is not recommended to enable backup route for a ring topology running RIP.

1.1.4 Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Enter the RIP routing configuration mode.
router rip

(4) (Optional) Enter the IPv4 VRF address family configuration mode.
address-family ipv4 vrf *vrf-name*

(5) Enable backup route.
enable backup-route

By default, backup route is disabled.

1.19 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	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 [**connected** | **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.
show ip rip rmflags	Displays global information about RIP.

Command	Purpose
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.
debug ip rip route	Debugs the route changes of the RIP process.

1.20 Configuration Examples

1.20.1 Building a RIP Routing Domain

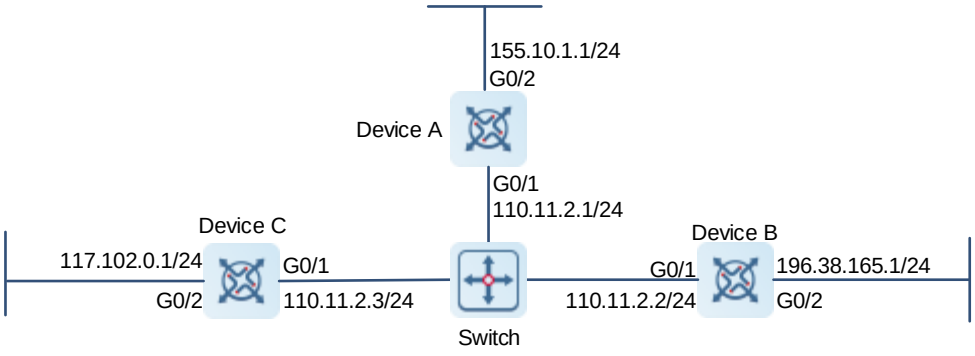
1. Requirements

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, 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    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 110.11.2.3, 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 110.11.2.2, 00:19:18, GigabitEthernet 0/1
```

- Device B

```
Device B# 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    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 110.11.2.3, 00:00:47, GigabitEthernet 0/1
```

- Device C

```
Device C# 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    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 110.11.2.2, 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.

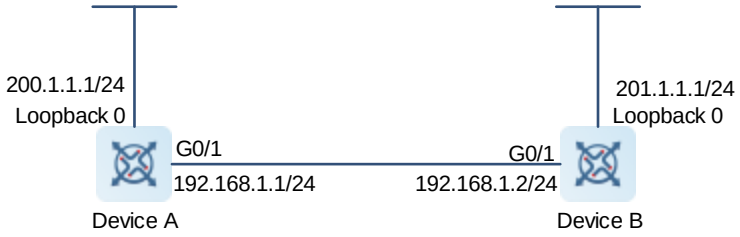
1.20.2 Configuring RIP to Prevent Route Loop

1. Requirements

Device A and Device B 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.

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
192.168.1.0/24    auto-summary
192.168.1.0/24
    [1] directly connected, GigabitEthernet 0/1
200.1.1.0/24    auto-summary
200.1.1.0/24
    [1] directly connected, Loopback 0
201.1.1.0/24    auto-summary
201.1.1.0/24
    [1] via 192.168.1.2 GigabitEthernet 0/1  03:01    permanent
```

- Device B

```
Device B# show ip rip database
192.168.1.0/24    auto-summary
192.168.1.0/24
    [1] directly connected, GigabitEthernet 0/1
200.1.1.0/24    auto-summary
200.1.1.0/24
    [1] via 192.168.1.1 GigabitEthernet 0/1  01:45    permanent
201.1.1.0/24    auto-summary
201.1.1.0/24
    [1] directly connected, Loopback 0
```

6. Configuration Files

- Device A configuration file

```
!
interface gigabitethernet 0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
 ip rip split-horizon poisoned-reverse
 ip rip triggered
!
interface loopback 0
 ip address 200.1.1.1 255.255.255.0
!
router rip
 network 192.168.1.0
 network 200.1.1.0
 graceful-restart
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
 no switchport
 ip address 192.168.1.2 255.255.255.0
 ip rip split-horizon poisoned-reverse
 ip rip triggered
!
interface loopback 0
 ip address 201.1.1.1 255.255.255.0
!
router rip
 network 192.168.1.0
 network 201.1.1.0
```

```
 graceful-restart
!
```

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.

1.20.3 Configuring External Routes Imported by RIP

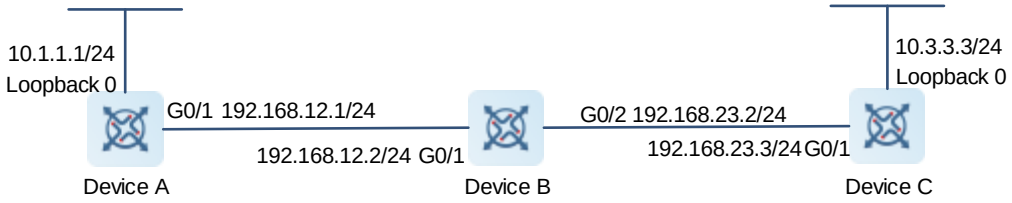
1. Requirements

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
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
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
!
```

1.20.4 Configuring Increasing the Metric of a RIP Interface

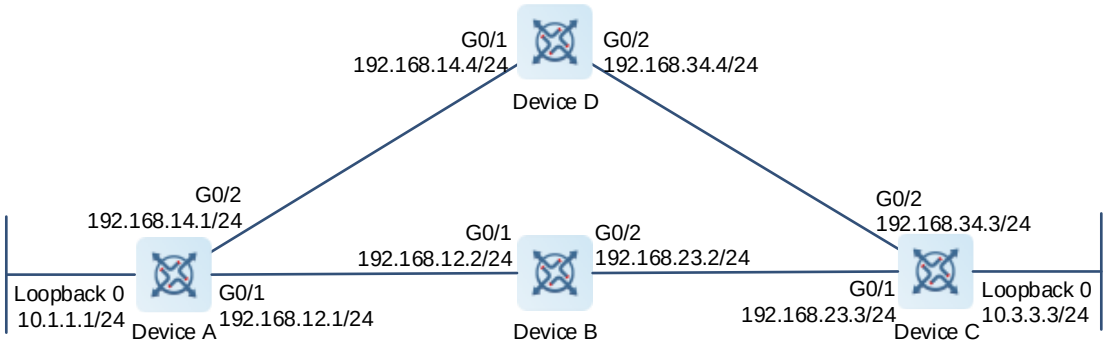
1. Requirements

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-List 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 [120/2] via 192.168.12.2, 00:06:11, GigabitEthernet 0/1
```

6. Configuration Files

Device C configuration file.

```
!
ip access-list standard 1
 10 permit 10.3.3.0 0.0.0.255
```

```
!
router rip
 offset-list 1 out 3 gigabitEthernet 0/2
!
```

1.20.5 Configuring RIP to Distribute a Summarized Route

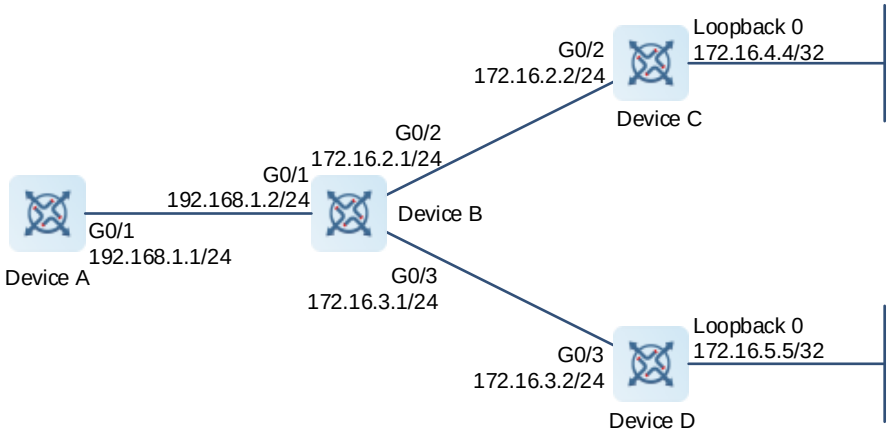
1. Requirements

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 [120/1] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1
```

6. Configuration Files

Device B configuration file.

```
!
interface gigabitethernet 0/1
ip rip summary-address 172.16.0.0 255.255.248.0
!
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 8
1.3.6 Configuring Split Horizon or Poison Reverse 8
1.3.7 Configuring a Passive Interface 9
1.4 Configuring RIPng Route Distribution 10
1.4.1 Overview 10
1.4.2 Configuration Tasks 10
1.4.3 Generating a Default Route 10
1.4.4 Configuring External Route Redistribution 11
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 12
1.6.1 Overview 12
1.6.2 Configuration Tasks 12
1.6.3 Configuring to Modify the Management Distance of an RIPng Route 12
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 13
1.7 RIPng Authentication 14
1.7.1 Overview 14
1.7.2 Restrictions and Guidelines 14
1.7.3 Procedure 14
1.8 Modifying Timers 15
1.8.1 Overview 15
1.8.2 Restrictions and Guidelines 15
1.8.3 Procedure 15
1.9 Enabling GR 15
1.9.1 Overview 15
1.9.2 Restrictions and Guidelines 15
1.9.3 Procedure 16
1.10 Configuring a Super VLAN to Enable RIPng 16
1.10.1 Overview 16
1.10.2 Restrictions and Guidelines 16
1.10.3 Procedure 16
1.11 Monitoring 17
1.12 Configuration Examples 17

1.12.1 Configuring Basic Functions of RIPng 17

1.12.2 Advertising Default Routes/External Routes 21

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

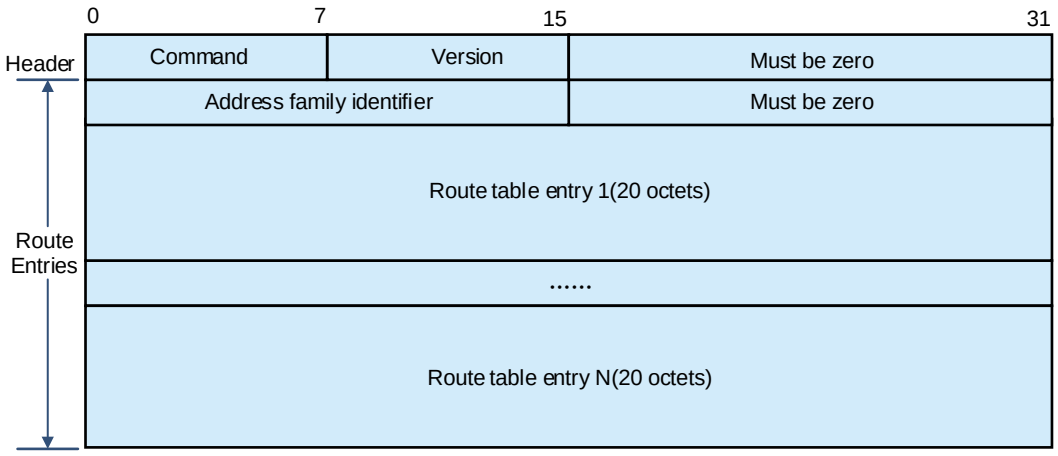
- IGP and EGP

  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

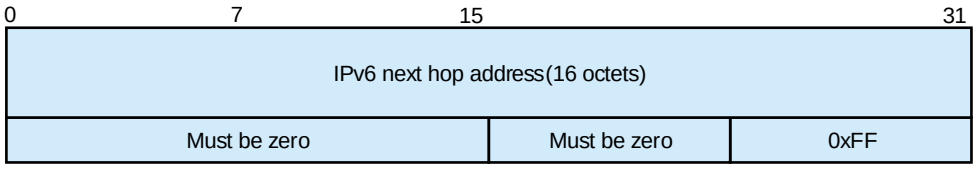
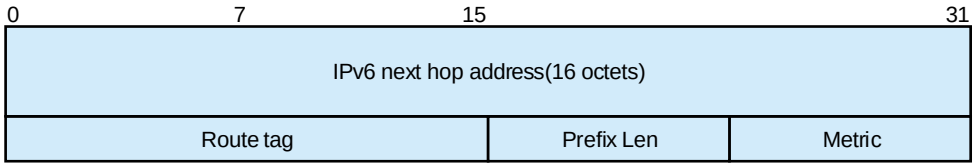


Figure 1-3 Format of IPv6 Prefix RTE



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

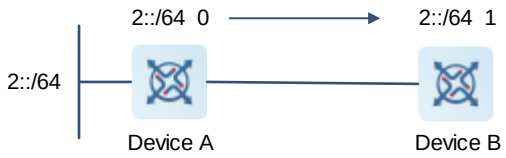
  RIPng is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance. The router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own 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

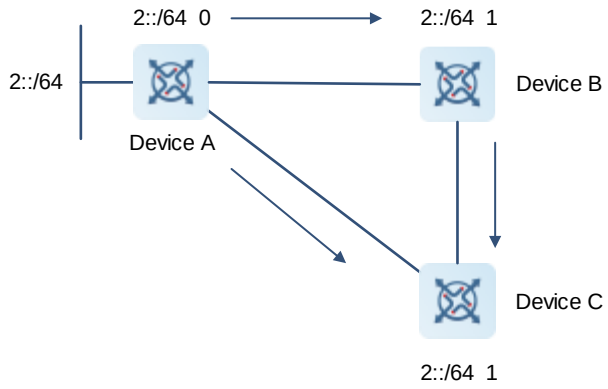


- Selecting the optimum route

  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

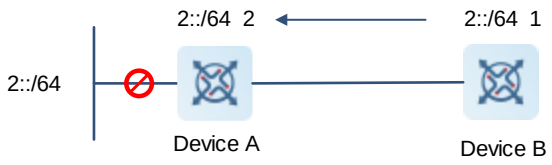
RIPng uses functions such as split horizon and poison reverse to avoid route loops.

- 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

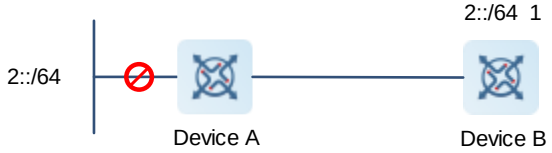


- Split horizon

  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



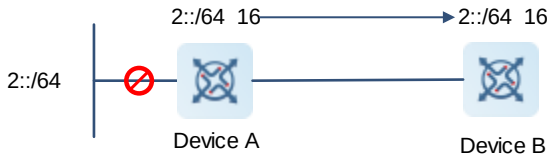
- Poison reverse

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



6. RIPng Authentication

IPv6 provides two authentication mechanisms, that is, authentication header (AH) and encapsulating security payload (ESP). RIPng use the authentication mechanisms to prevent routers that access the network illegally and hosts that forge RIPng packets from participating in RIPng routing switching. RIPng packets received on the RIPng interface are authenticated and decrypted. If authentication or decryption fails, the packets are dropped and do not participate in route learning.

Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. At present, RIPng authentication is implemented by associating with the security association (SA) authentication of IPsec. SA defines a set of security algorithms and keys to ensure IP security. If a service is associated with IPsec SA authentication, the RIPng service will use an SA authentication key to authenticate and encrypt packets. For example, the definition of SM3 (OSCCA algorithm) authentication is added to SA authentication. For the RIPng service, only the SA authentication needs to be associated to encrypt/decrypt packets using SM3 authentication keys.

1.1.3 Protocols and Standards

- RFC 2080: 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) RIPng Authentication

(6) (Optional) Modifying Timers

(7) (Optional) Enabling GR

(8) (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 the RIPng routing 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 the RIPng 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 the routing 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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 RIPng routing configuration mode.

ipv6 router rip

(4) Configure split horizon.

split-horizon [**poison-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 RIPng routing 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

- Enter the Loopback interface configuration mode.

  interface loopback *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 RIPng routing configuration mode.

ipv6 router rip

(4) Generate a default route.

redistribute { **connected** | **ospf** process-id **| static** } [**metric** *metric-value* | **route-map** *route-map-name*] *

By default, the function of redistributing routes from other routing domains to RIPng is not configured.

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 RIPng routing configuration mode.

ipv6 router rip

(5) Configure to filter the sent and 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 a 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 RIPng routing 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the interface metric value of the 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 RIPng routing 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 RIPng Authentication

1.7.1 Overview

All the routers connected to the RIPng network must be authenticated so as to ensure stability of the RIPng network and protect the network against intrusions.

1.7.2 Restrictions and Guidelines

- The RIPng basic functions must be configured.
- If authentication is configured in process configuration mode, the configuration takes effect on all the interfaces of the process.
- If authentication is configured in both process and interface configuration modes, the interface-based configuration takes effect preferentially.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIPng routing configuration mode.

ipv6 router rip

(4) (Optional) Associate a RIPng routing process with SA authentication.

ipsec sa *sa-name*

By default, RIPng routing processes are not associated with SA authentication.

(5) Exit the RIPng routing process.

exit

(6) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(7) Associate SA authentication with an interface or cancel SA authentication for an interface.

ipv6 rip ipsec sa { **disable** | *sa-name* }

SA authentication is not configured on an interface by default.

1.8 Modifying Timers

1.8.1 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.

1.8.2 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.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIPng routing 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.

1.9 Enabling GR

1.9.1 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.

1.9.2 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.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the RIPng routing configuration mode.

ipv6 router rip

(4) Enable GR.

graceful-restart [**grace-period** *grace-period*]

The GR function is enabled by default.

1.10 Configuring a Super VLAN to Enable RIPng

1.10.1 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.

1.10.2 Restrictions and Guidelines

- The RIPng basic functions must be configured.
- The designated sub VLAN must be connected to neighbors.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the SVI interface configuration mode.

interface vlan *interface-number*

(4) Enable RIPng on a super VLAN.

ipv6 rip subvlan [**all |** *vlan-id*]

By default, the RIPng function is disabled on a super VLAN.

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.

Table 1-2 Monitoring

Command	Purpose
show ipv6 rip	Displays information about the RIPng process.
show ipv6 rip database	Displays the RIPng routing table.
show ipv6 rip rmflags	Displays global information about RIPng.
debug ipv6 rip [interface *interface-type interface-number* | **nsm** | **restart** | **event** [**ipsec**]]	Debugs RIPng.

1.12 Configuration Examples

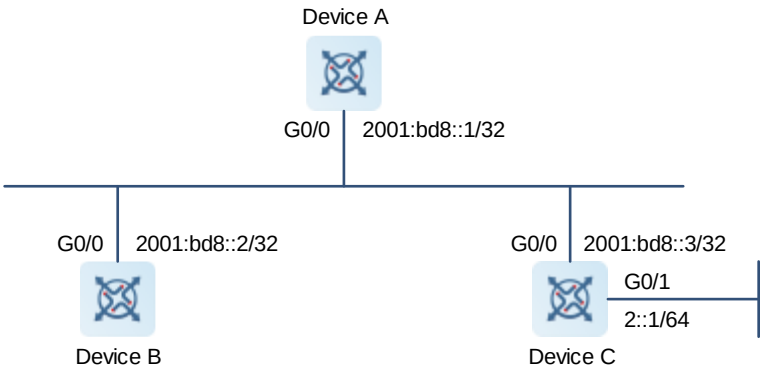
1.12.1 Configuring Basic Functions of RIPng

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/0
DeviceA(config-if-GigabitEthernet 0/0)# no switchport
DeviceA(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32
DeviceA(config-if-GigabitEthernet 0/0)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/0
DeviceB(config-if-GigabitEthernet 0/0)# no switchport
DeviceB(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32
DeviceB(config-if-GigabitEthernet 0/0)# exit
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface gigabitethernet 0/0
DeviceC(config-if-GigabitEthernet 0/0)# no switchport
DeviceC(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32
DeviceC(config-if-GigabitEthernet 0/0)# exit
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# no switchport
```

```
DeviceC(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

(2) Enable the RIPng routing function on all the devices.

Configure Device A.

```
DeviceA(config)# ipv6 router rip
DeviceA(config-router)# exit
DeviceA(config)# interface gigabitethernet 0/0
DeviceA(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

Configure Device B.

```
DeviceB(config)# ipv6 router rip
DeviceB(config-router)# exit
DeviceB(config)# interface gigabitethernet 0/0
DeviceB(config-if-GigabitEthernet 0/0)# ipv6 rip enable
```

Configure Device C.

```
DeviceC(config)# ipv6 router rip
DeviceC(config-router)# exit
DeviceC(config)# interface gigabitethernet 0/0
DeviceC(config-if-GigabitEthernet 0/0)# ipv6 rip enable
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(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.

```
DeviceA# 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, EV - BGP EVPN, N - Nd to host

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.

```
DeviceB# 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, EV - BGP EVPN, N - Nd to host

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.

```
DeviceC# 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, EV - BGP EVPN, N - Nd to host

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
 no switchport
 ipv6 address 2001:db8::1/32
 ipv6 rip enable
!
```

- Device B configuration file

```
!
ipv6 router rip
```

```
!
interface gigabitethernet 0/0
 no switchport
 ipv6 address 2001:db8::2/32
 ipv6 rip enable
!
```

- Device C configuration file

```
!
ipv6 router rip
!
interface gigabitethernet 0/0
 no switchport
 ipv6 address 2001:db8::3/32
 ipv6 rip enable
!
interface gigabitethernet 0/1
 no switchport
 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.

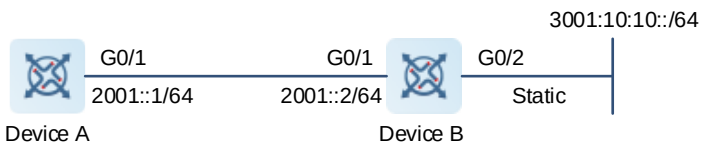
1.12.2 Advertising Default Routes/External Routes

1. Requirements

On a network adopting RIPng 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.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 router rip
DeviceB(config-router)# redistribute static
```

(2) Configure redistribution of a default route on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(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

```
DeviceA# show ipv6 route rip
IPv6 routing table name - Default - 1 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, EV - BGP EVPN, N - Nd to host

R     3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
```

- Device B

```
DeviceB# show ipv6 route rip

IPv6 routing table name - Default - 1 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 OSPFv2 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Basic Concepts 2

1.1.3 OSPF Working Process 14

1.1.4 OSPF Routing 15

1.1.5 OSPF Route Advertisement 16

1.1.6 OSPF Route Summarization 17

1.1.7 OSPF Route Filtering 17

1.1.8 Enhanced Security and Reliability 17

1.1.9 Network Management Functions 21

1.1.10 Protocols and Standards 21

1.2 Configuration Task Summary 21

1.3 Configuring Basic Features 24

1.3.1 Overview 24

1.3.2 Restrictions and Guidelines 24

1.3.3 Configuration Tasks 25

1.3.4 Configuring OSPF Process 25

1.3.5 Configuring Router ID 25

1.3.6 Enabling OSPF on a Network Segment 26

1.3.7 Enabling OSPF on an Interface 27

1.3.8 Creating a Virtual Link....28
1.4 Configuring OSPF Network Type....29
1.4.1 Overview....29
1.4.2 Restrictions and Guidelines....29
1.4.3 Configuration Tasks....29
1.4.4 Configuring the Interface Network Type....30
1.4.5 Configuring a Neighbor....31
1.4.6 Configuring the Interface Priority....31
1.4.7 Disabling Source Address Verification....32
1.5 Configuring Stub and NSSAs....33
1.5.1 Overview....33
1.5.2 Restrictions and Guidelines....33
1.5.3 Configuration Tasks....34
1.5.4 Configuring a Stub Area....34
1.5.5 Configuring an NSSA....35
1.6 Adjusting OSPF Routing....36
1.6.1 Overview....36
1.6.2 Restrictions and Guidelines....36
1.6.3 Configuration Tasks....36
1.6.4 Configuring the AD....36
1.6.5 Configuring the Reference Bandwidth....37
1.6.6 Configuring the Cost of an Interface....38
1.6.7 Configuring Cost Fallback Value for an AP....39

1.6.8 Configuring the Cost of the Default Route in a Stub Area or an NSSA....39
1.6.9 Configuring the Default Metric Value for Redistribution....40
1.6.10 Configuring the Maximum Metric....41
1.6.11 Configuring RFC 1583 Compatibility....42
1.6.12 Configuring Association of External Route Forwarding Addresses with Interface Configuration....42
1.7 Configuring OSPF Route Advertisement....43
1.7.1 Overview....43
1.7.2 Restrictions and Guidelines....44
1.7.3 Configuration Tasks....44
1.7.4 Configuring External Route Redistribution....44
1.7.5 Generating a Default Route....45
1.7.6 Configuring a Device as ASBR....46
1.8 Configuring OSPF Route Summarization....46
1.8.1 Overview....46
1.8.2 Restrictions and Guidelines....46
1.8.3 Configuration Tasks....47
1.8.4 Configuring Inter-Area Route Summarization....47
1.8.5 Configuring External Route Summarization....48
1.8.6 Configuring a Discard Route....49
1.9 Configuring OSPF Route Filtering....49
1.9.1 Overview....49
1.9.2 Restrictions and Guidelines....49

1.9.3 Configuration Tasks 50
1.9.4 Configuring a Passive Interface 50
1.9.5 Disabling Interfaces from Sending OSPF Packets 50
1.9.6 Configuring Inter-area Route Filtering 51
1.9.7 Configuring Redistributed Route Filtering 52
1.9.8 Configuring Learned Route Filtering 53
1.10 Adjusting OSPF Network Convergence Speed 54
1.10.1 Overview 54
1.10.2 Restrictions and Guidelines 54
1.10.3 Configuration Tasks 54
1.10.4 Configuring the Hello Interval 55
1.10.5 Configuring the Dead Interval 55
1.10.6 Configuring LSU Transmission Delay 56
1.10.7 Configuring LSU Retransmission Interval 57
1.10.8 Configuring LSU Generation Time 58
1.10.9 Configuring LSA Group Refresh Time 59
1.10.10 Configuring LSA Group Refresh Interval 60
1.10.11 Configuring Duplicate LSA Receiving Delay 60
1.10.12 Configuring Inter-Area Route Computation Delay 61
1.10.13 Configuring External Route Computation Delay 61
1.10.14 Configuring SPF Computation Delay 62
1.10.15 Enabling Two-Way Maintenance 63
1.11 Configuring OSPF Authentication 63

1.11.1 Overview 63
1.11.2 Restrictions and Guidelines 64
1.11.3 Configuration Tasks 64
1.11.4 Configuring the Authentication Type of an Area 64
1.11.5 Configuring the Authentication Type of an Interface 65
1.11.6 Configuring a Plain Text Authentication Key for an Interface 66
1.11.7 Configuring an MD5 Authentication Key for an Interface 67
1.12 Enabling Fast Reroute 68
1.12.1 Overview 68
1.12.2 Restrictions and Guidelines 68
1.12.3 Configuration Tasks 68
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 72
1.13.3 Configuration Tasks 72
1.13.4 Configuring the Maximum Number of Concurrent Neighbors on the Current Process 72
1.13.5 Configuring the Maximum Number of Concurrent Neighbors on All Processes 72
1.14 Configuring the GR Function 73
1.14.1 Overview 73
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 76
1.15.5 Configuring BFD Correlation with OSPF Globally 77
1.16 Enabling Overflow 77
1.16.1 Overview 77
1.16.2 Restrictions and Guidelines 77
1.16.3 Configuration Tasks 77
1.16.4 Configuring the Memory Overflow Function 78
1.16.5 Configuring the Database Overflow Function 78
1.16.6 Configuring the External LSA Database Overflow Function 79
1.17 Configuring Network Management Functions 80
1.17.1 Overview 80
1.17.2 Restrictions and Guidelines 80
1.17.3 Configuration Tasks 80
1.17.4 Binding the MIB with an OSPF Process 80
1.17.5 Configuring the Trap Function 81
1.17.6 Configuring the Logging Function 82

1.18 Enabling NSR 82
1.18.1 Overview 82
1.18.2 Restrictions and Guidelines 82
1.18.3 Procedure 83
1.19 Enabling the iSPF Feature 83
1.19.1 Overview 83
1.19.2 Restrictions and Guidelines 83
1.19.3 Procedure 83
1.20 Configuring to Disable MTU Verification 84
1.20.1 Overview 84
1.20.2 Restrictions and Guidelines 84
1.20.3 Procedure 84
1.21 Configuring to Enable Conflict Detection of Type-4 LSAs 85
1.21.1 Overview 85
1.21.2 Restrictions and Guidelines 85
1.21.3 Procedure 85
1.22 Configuring a Super VLAN to Enable OSPF 85
1.22.1 Overview 85
1.22.2 Restrictions and Guidelines 86
1.22.3 Procedure 86
1.23 Monitoring 86
1.24 Configuration Examples 89
1.24.1 Configuring Basic Functions of OSPF 89

1.24.2 Configuring a Stub Area....94
1.24.3 Configuring an NSSA....96
1.24.4 Correlating OSPF Process with BFD....99
1.24.5 Configuring Fast Reroute....101
1.24.6 Configuring Network Management Functions....102
1.24.7 Configuring a Virtual Link....105
1.24.8 Selecting a DR of OSPF....107

1 Configuring OSPFv2

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 OSPF Version 2.

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 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 on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

2. 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.

3. 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. To prevent conflicts between Router IDs obtained by different routers through automatic selection, 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.

4. Area

An area is a logical group of routers, and each group is identified by an area ID. As shown in Figure 1-1, OSPF supports dividing the network topology into multiple areas, which can alleviate the computing pressure of large-scale networks.

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.

OSPF areas can be classified into following types:

- 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 a 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). ABR only advertises a 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 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.

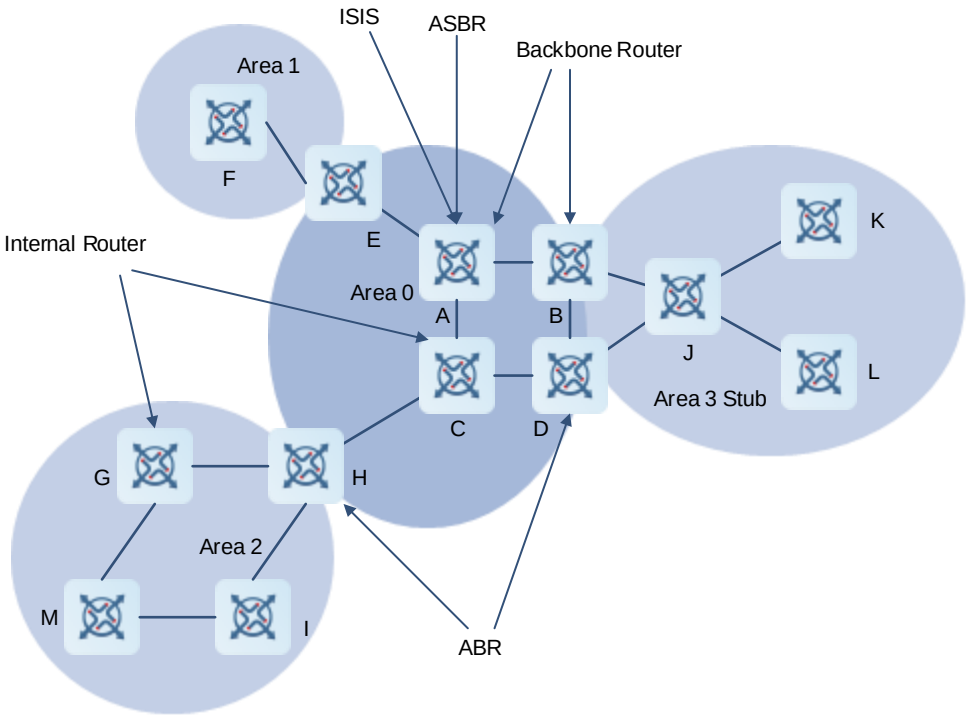
- Totally not-so-stubby area (NSSA)

  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 configured as 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 Types of OSPF Areas and Routers



5. OSPF Router Types

The following types of routers are defined in OSPF, and assigned with different responsibilities:

- Internal router

  All interfaces of an interval router belong to the same 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 area. It may be a router inside an area, or an ABR. See A shown in Figure 1-1.

6. LSA

OSPF encapsulates and advertises the description of routing information through a Link State Advertisement (LSA). Common LSA types are shown in Table 1-1.

Table 1-1 OSPF LSA Types

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.

The format of LSA packet header is described as follows.

Figure 1-2 LSA Packet Header Format

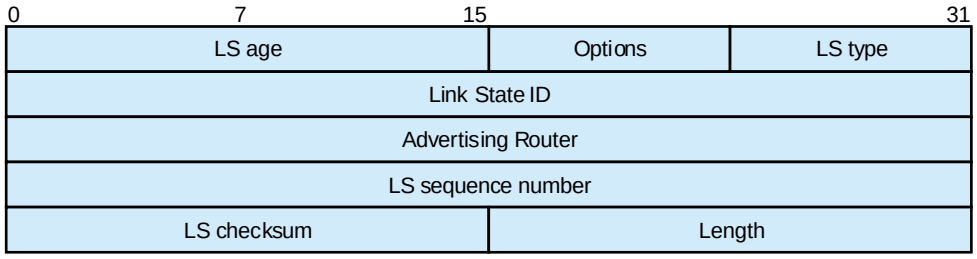


Table 1-2 shows the support of various areas for different types of LSAs. Stub area, NSSA, Totally Stub area, and Totally NSSA, as special forms of conventional areas, help reduce the number of LSAs transferred in the OSPF area, eliminate the propagation of a large number of Type 3 LSAs and Type 5 LSAs in the area, reduce the burden on routers, and enhance the stability of OSPF routing.

Table 1-2 Support of LSAs by Different Areas

Area	Type1 and Type 2	Type 3	Type 4	Type 5	Type 7
Non-Stub/Totally Stub and NSSA/Totally NSSAs	Allowed	Allowed	Allowed	Allowed	Blocked
Stub Area	Allowed	Allowed, including one default route	Blocked	Blocked	Blocked
Totally Stub Area	Allowed	Only one default route is allowed	Blocked	Blocked	Blocked

Area	Type1 and Type 2	Type 3	Type 4	Type 5	Type 7
NSSA	Allowed	Allowed, including one default route	Allowed	Blocked	Allowed
Totally NSSA	Allowed	Only one default route is allowed	Allowed	Blocked	Allowed

Note

ABR advertises a default route to Stub/Totally Stub and NSSA/Totally NSSAs using a Type 3 LSA.

ABR converts Type 7 LSA to Type 5 LSA in NSSA/Totally NSSA, and advertise the route to the backbone area.

7. 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:

OSPF involves the following five types of packets, as shown in Table 1-3.

Table 1-3 Types of OSPF Packets

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
DD	DD (Database Description) packets carry brief information about the local LSDB and are used to synchronize the LSDBs between OSPF neighbors.
LSR	LSR (Link State Request) 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 (Link State Update) packets are used to send the required LSAs to peers.
LSAck	LSAck (Link State Acknowledgment) packets are used to acknowledge the received LSAs.

Format of OSPF packets is shown in the figure below.

Figure 1-3 Format of OSPF Packets

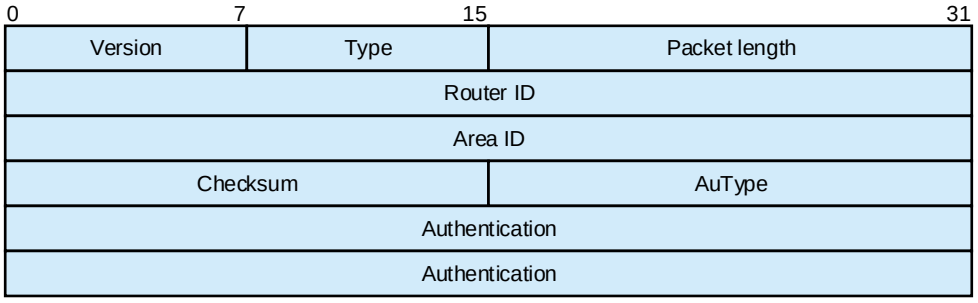


Table 1-4 Description of OSPF Packet Format Fields

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.

8. 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.

- 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.

- 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. 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.

Configuring an area as a Stub/Totally Stub area or NSSA/Totally NSSA can reduce a large number of E1, E2, and IA routes in the routing table of routers in the area.

Table 1-5 Route Types in a Stub/NSSA

Area	Routes in the routing table of routers in the area
Non-Stub/Totally Stub, and NSSA/Totally NSSA	O: Route to a destination network in the local area. IA: Route to a destination network in another area. E1 or E2: Route or default route to a destination network outside the AS through any ASBR in the AS.
Stub area	O: Route to a destination network in the local area. IA: Route to a destination network in another area.
Totally Stub area	O: Route to a destination network in the local area. IA: Default route.
NSSA	O: Route to a destination network in the local area. IA: Route to a destination network in another area. N1or N2: Route or default route to a destination network outside the AS through any ASBR in the area.
Totally NSSA	O: Route to a destination network in the local area. IA: Default route. N1or N2: Route or default route to a destination network outside the AS through any ASBR in the area.

9. OSPF Neighbor State

On the OSPF network, neighbor devices need to reach the adjacency state before exchanging link information. Any two devices form an OSPF neighborhood relation or adjacency relation.

- Neighborhood: If two routers can send and receive Hello packets from each other, and can successfully negotiate the parameters carried in the Hello packets, then they are neighbors to each other.
- Adjacency: When neighbor devices successfully exchange LSA and realize LSDB synchronization, then an adjacency relation is successfully established.

Table 1-7shows the 8 OSPF neighbor states.

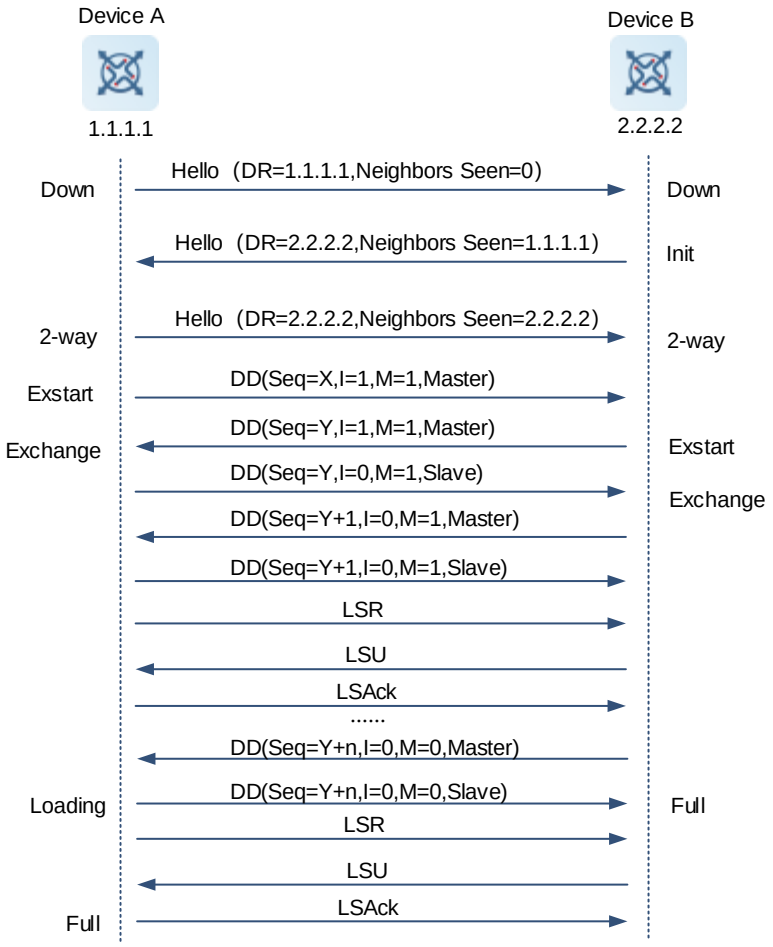
Table 1-6 OSPF Neighbor State Machine and Description

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.

State	Description
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 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 shows the OSPF adjacency establishment process on the broadcast network. When the neighbor state is Full, the adjacency is established.

Figure 1-4 OSPF Adjacency Establishment Process on Broadcast Network



10. 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 shownFigure 1-5 and Figure 1-6

Figure 1-5 Number of Adjacency Relationships Before DR Election

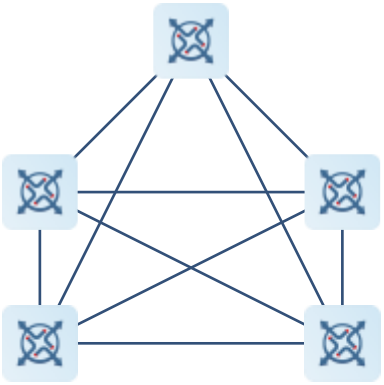
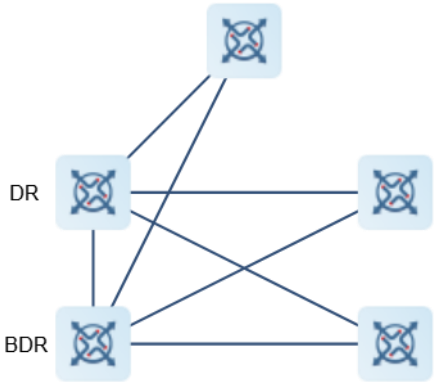


Figure 1-6 Number of Adjacency Relationships After DR Election



11. 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 1-7 Introduction to OSPF Network Types

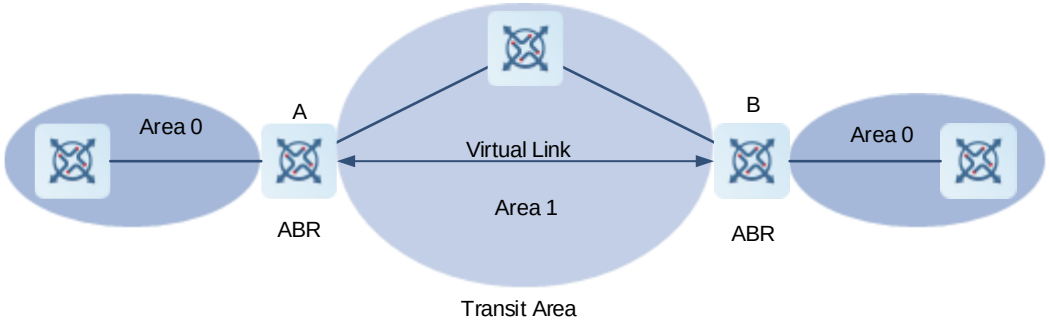
Network Type	Link Layer Protocol	Neighbor Relationship and DR Election
Broadcast	Ethernet and FDDI belong to the broadcast network type by default.	● Neighbors are discovered, and the DR and BDR are elected. ● The DR or BDR exchanges LSAs with all other routers to set up an adjacency. ● Except the DR 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.

12. Virtual Links

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.

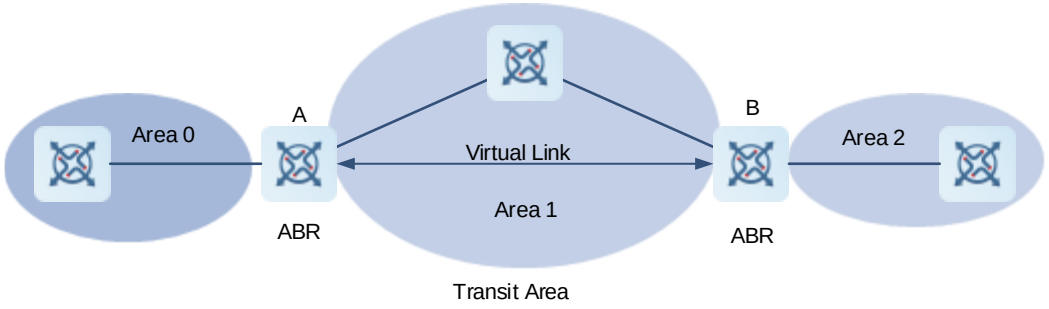
A virtual link relies on an OSPF intra-domain route, making two ABRs adjacent. The OSPF packet information exchanged by ABRs is transparent to the intermediate device.

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.

1.1.3 OSPF Working Process

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.

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, subnet mask, authentication information, Hello interval and 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.

(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.

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.

(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.

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.

1.1.4 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 administrative distance

  The administrative 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 1-8 Routing Protocols and Default Administrative 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

1.1.5 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.

1.1.6 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.

1.1.7 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.

1.1.8 Enhanced Security and Reliability

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

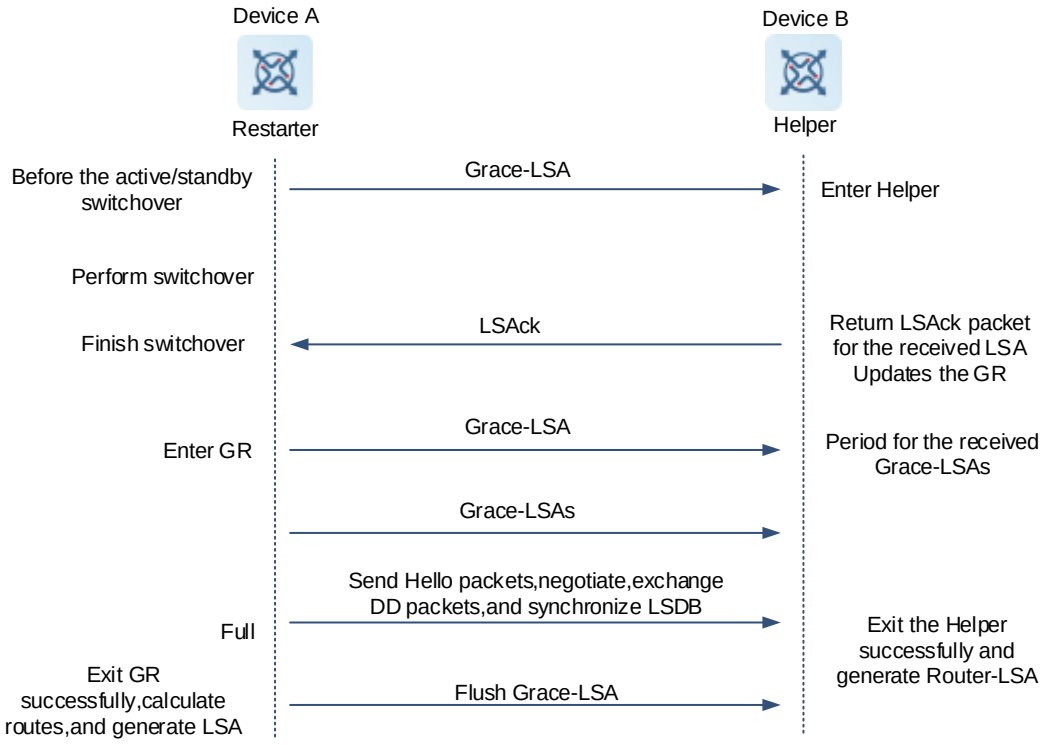
When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

7. 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.

8. 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, or OSPF 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.

9. iSPF Feature

- The Open Shortest Path First (OSPF) topology is area based. The Shortest Path First (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.

10. 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 fast hello function, correlation with BFD, or OSPF fast reroute function to speed up network convergence.

1.1.9 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.

1.1.10 Protocols and Standards

- RFC 2328: OSPF Version 2
- RFC 2370: The OSPF Opaque LSA Option
- RFC 3137: OSPF Stub Router Advertisement
- RFC 3623: Graceful OSPF Restart
- RFC 3630: Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 3682: The Generalized TTL Security Mechanism (GTSM)
- RFC 4750: OSPF Version 2 Management Information Base

1.2 Configuration Task Summary

The OSPFv2 configuration includes the following tasks:

(1) Configuring Basic Features

- Configuring OSPF Process

- (Optional) Configuring Router ID
- Enable OSPF by performing at least one of the following configuration tasks:
- Enabling OSPF on a Network Segment

  Enabling OSPF on an Interface
- (Optional) Creating a Virtual Link

(2) (Optional) Configuring OSPF Network Type

- Configuring the Interface Network Type
- (Optional) Configuring a Neighbor
- (Optional) Configuring the Interface Priority
- (Optional) Disabling Source Address Verification

(3) (Optional)Configuring Stub and NSSAs The following tasks are optional. Select tasks for configuration according to actual condition.

- Configuring a Stub Area
- Configuring an NSSA

(4) (Optional) The following tasks 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 RFC 1583 Compatibility
- Configuring Association of External Route Forwarding Addresses with Interface Configuration

(5) (Optional)Configuring OSPF Route Advertisement

- Configuring External Route Redistribution
- Generating a Default Route
- (Optional) Configuring a Device as ASBR

(6) (Optional)Configuring OSPF Route Summarization. The following tasks are optional. Select tasks for configuration according to actual condition.

- Configuring Inter-Area Route Summarization
- Configuring External Route Summarization
- Configuring a Discard Route

(7) (Optional)Configuring OSPF Route Filtering. The following tasks are optional. Select tasks for configuration according to actual condition.

- Configuring a Passive Interface
- Disabling Interfaces from Sending OSPF Packets
- Configuring Inter-area Route Filtering
- Configuring Redistributed Route Filtering
- Configuring Learned Route Filtering

(8) (Optional)Adjusting OSPF Network Convergence Speed. The following tasks 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

(9) (Optional)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) (Optional)Enabling Fast Reroute

- Configuring Fast Reroute
- (Optional)Configuring Interface LFA Protection
- (Optional)Preventing an Interface From Becoming a Backup Interface

(11) (Optional)Modifying the Maximum Number of Concurrent Neighbors. The following tasks 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

(12) (Optional)Configuring the GR Function. The following tasks are optional. Select tasks for configuration according to actual condition.

- Enabling the GR Function
- Configuring the OSPF GR Helper Function

(13) (Optional)Correlating OSPF with BFD. The following tasks are optional. Select tasks for configuration according to actual condition.

- Configuring BFD Correlation with OSPF on an Interface
- Configuring BFD Correlation with OSPF Globally

(14) (Optional)Enabling Overflow. The following tasks 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

(15) (Optional)Configuring Network Management Functions. The following tasks are optional. Select tasks for configuration according to actual condition.

- Binding the MIB with an OSPF Process
- Configuring the Trap Function
- Configuring the Logging Function

(16) (Optional)Enabling NSR

(17) (Optional)Enabling the iSPF Feature

(18) (Optional)Configuring to Disable MTU Verification

(19) (Optional)Configuring to Enable Conflict Detection of Type-4 LSAs

(20) (Optional)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.
- When OSPFis 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) Enable OSPF by performing at least one of the following configuration tasks:

Enabling OSPF on a Network Segment

Enabling OSPF on an Interface

(4) (Optional) Creating a Virtual Link

1.3.4 Configuring OSPF Process

1. Overview

To enable OSPF on the device, the OSPF process must be created by specifying the process ID.

2. Restrictions and Guidelines

- OSPF supports multiple instances. 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

No OSPF process is created by default.

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.
- Different OSPF processes on the same router must have different Router IDs.
- When a router ID is not manually configured, OSPF automatically 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 routing 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 Enabling OSPF on a Network Segment

1. Overview

To realize interaction of OSPF routing information between devices, interfaces of the devices must be added to the OSPF process. Through enabling OSPF on a network segment, all interfaces whose IP addresses fall within the range of the network segment join the OSPF process, and are associated with the area.

2. Restrictions and Guidelines

- All routers running OSPF must be configured to join interfaces into the OSPF process.

  When an interface IP address matches the IP address range defined by the **network area** command of multiple OSPF processes at the same time, the OSPF process that the interface joins will be determined by the optimal matching method.
- When both the **network area** command in the OSPF process configuration mode, and the **ip ospf area** command in the interface configuration mode are configured, the latter will prevail.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enable OSPF on the network segment, 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

1. Overview

To realize interaction of OSPF routing information between devices, interfaces of the devices must be added to the OSPF process. By enabling OSPF on the specified interface, all IP addresses under the interface will automatically join the OSPF process, and be associated with the area.

2. Restrictions and Guidelines

- The configuration is mandatory for each 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

(5) Allow the interface to generate OSPF packets.

no ip ospf disable all

By default, an interface is allowed to generate OSPF packets.

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.
- The current OSPF version supports AES128 encryption and simple encryption. When encryption authentication is enabled globally, AES128 encryption algorithm is preferred for key encryption. If the OSPF plain-text authentication encryption key is configured through the keyword **authentication-key** command, the maximum length of the AES128 encryption key is 21 characters, and the maximum length of the simple encryption key is 18 characters. If the MD5 ciphertext authentication key is configured through the keyword **message-digest-key** command, the maximum length of the AES128 encryption key is 33 characters, and the maximum length of the simple encryption key is 34 characters. You are advised to configure the AES128 encryption key because AES128 encryption is more secure.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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

There are five OSPF network types. 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. This configuration allows you to forcibly modify the network type of the interface.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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 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 routing 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. 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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 Configuring Stub and NSSAs

1.5.1 Overview

Configuring a stub area as the Stub area or NSSA helps to reduce the amount of routing information interaction, reduce the size of the routing table, and enhance routing stability.

1.5.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- A backbone area and transmission area cannot be configured as a Stub area or NSSA.

- Routers in the Stub area cannot import external routes, while routers in the NSSA can import external routes.

1.5.3 Configuration Tasks

The configuration includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Configuring a Stub Area
- Configuring an NSSA

1.5.4 Configuring a Stub Area

1. Overview

Stub area is the stub area of OSPF. Configuring a Stub Area can reduce the number of LSAs in the area. The ABR router in the Stub area will not transmit Type 5 LSAs (external routes), but will also advertise a default route to the Stub area.

Totally Stub area is a totally stub area, which is an upgrade of the Stub area. Routers in the Totally Stub area will not transmit Type 3 LSAs (inter-domain routes) and Type 5 LSAs (external routes). The ABR will only advertise a default route to the Stub area.

To reduce the size of the routing table of the routers in the area, you can configure a Stub area or Totally Stub area.

2. Restrictions and Guidelines

- The area must be configured as Stub area on all routers in the area.
- To configure a Totally Stub area, you only need to select the **no-summary** keyword when running the **area stub** command on the ABR. The routing devices in the Totally Stub area can only learn the routes in the area and the internal default routes generated by the ABR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configuring a Stub Area.

area *area-id* **stub** [**no-summary**]

By default, the Stub area function is disabled.

1.5.5 Configuring an NSSA

1. Overview

NSSA is similar to the Stub area, but allows ASBR. ASBR redistributed routes will be transmitted in the NSSA in the form of a Type 7 LSA. On the ABR, the Type 7 LSA is converted to Type 5 LSA and then transmitted to other areas. This ABR is also called the translator. The ABR will also advertise the default route to the NSSA.

Totally NSSA area is an upgrade of NSSA. Compared with routers in the NSSA, routers in the Totally NSSA can only advertise a default inter-domain route, and other Type 3 LSAs (inter-domain routes) are not allowed to be transmitted.

You are advised to configure NSSA or Totally NSSA if you want to reduce the size of the routing table of routers in the area and the number of LSAs in the area, and to import OSPF routes outside the area.

2. Restrictions and Guidelines

- The area must be configured as NSSA on all routers in the area.
- When the **default-information-originate** parameter is executed on the ABR of the NSSA, the Type 7 LSA default route will be generated regardless of whether there is a default route in the route table. When this parameter is executed on the ASBR (also not an ABR) of the NSSA, the Type 7 LSA default route will be generated only if there is a default route in the route table.
- Configuring a Totally NSSA area can further reduce the number of LSAs sent to the NSSA. If the **no-summary** attribute is configured on the ABR, the ABR will be prevented from sending summary LSA (Type 3 LSA) to the NSSA.
- In one NSSA, you are advised to specify only one ABR as the translator.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configuring an NSSA.

area *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translate type7 suppress-fa** | **translator** { **always** | **stability-interval** *stability-interval* } * | **zero-address-forwarding**] *

By default, the NSSA function is disabled.

1.6 Adjusting OSPF Routing

1.6.1 Overview

Configuring routing parameters such as administrative distance, reference bandwidth, and interface cost, can change the order in which routers select various routes to increase or decrease the priority of OSPF routes, and change OSPF routes to allow traffic to pass through or bypass certain nodes.

1.6.2 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.

1.6.3 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 RFC 1583 Compatibility
- Configuring Association of External Route Forwarding Addresses with Interface Configuration

1.6.4 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure an AD.

distance { *distance* [**route-map** *map-name*] | **ospf** { **external** *distance* [**route-map** *map-name*] | **inter-area** *distance* [**route-map** *map-name*] | **intra-area** *distance* [**route-map** *map-name*] } * }

By default, the administrative distance is **110** for all the OSPF routes.

1.6.5 Configuring the Reference Bandwidth

1. Overview

The default value of OSPF reference bandwidth is 100 Mbps, and the cost is the reference bandwidth divided by interface 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the reference bandwidth.

auto-cost reference-bandwidth *reference-bandwidth*

By default, the reference bandwidth value of interface metric calculation is 100 Mbps.

1.6.6 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. You are advised to configure a lower cost for a specific interface if you wish to manually specify a preferential line.
- Run the **auto-cost** command to configure 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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).

1.6.7 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.

- Enter the Layer 3 aggregate interface configuration mode.

interface aggregateport *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.

1.6.8 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 routing 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.

1.6.9 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 routing 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.

1.6.10 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:
  - 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the maximum metric.

max-metric router-lsa [**external-lsa** [*max-metric-value*] | **on-neighborup** [*full-interval-time*] | **include-stub** | **on-startup** [*startup-interval-time*] | **summary-lsa**

By default, the LSAs of normal metric are advertised.

1.6.11 Configuring RFC 1583 Compatibility

1. Overview

When there are multiple paths to an ASBR or the forwarding address of an external route, RFC 1583 and RFC 2328 define different routing rules. If RFC 1583 compatibility is configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC 1583 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure compatible RFC 1583.

compatible rfc1583

The RFC1583 rule function is enabled by default.

1.6.12 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure association of external route forwarding addresses with interface configuration.

commpatible forward-address

By default, the external route forwarding address is set according to the default rules.

1.7 Configuring OSPF Route Advertisement

1.7.1 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.

1.7.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

1.7.3 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

1.7.4 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 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 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure external route redistribution.

redistribute { **arp**-**host** | **connected** | **ospf** process-id [**match** { **externa**l [**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.

1.7.5 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 routing 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.

1.7.6 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a device as ASBR.

asbr enable

ASBR is disabled by default.

1.8 Configuring OSPF Route Summarization

1.8.1 Overview

Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes. Shield or filter routes.

1.8.2 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.

1.8.3 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

1.8.4 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 routing 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.

1.8.5 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure external route summarization.

summary-address *ipv4-address mask* [**not-advertise** | [**tag** *tag-value* | **cost** *cost* | **distribute-delay** *interval* | **nssa-only**] *]

The route summarization function is disabled by default.

1.8.6 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure a discard route.

discard-route { **external** | **internal** }

The discard route adding function is enabled by default.

1.9 Configuring OSPF Route Filtering

1.9.1 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.

1.9.2 Restrictions and Guidelines

The OSPF basic functions must be configured.

- There are three ways to implement route filtering:
  - Run the **passive-interface** command to configure the interface as a passive interface so that the interface no longer receives and sends Hello packets.
  - Run the **distribute-list out** command when the ASBR imports external routes, and you want to filter the imported external routes.
  - If it is necessary to restrict users' access to the specified destination network, run the **distribute-list in** command to filter the routes calculated by the received LSA. Only the routes that meet the filtering conditions can be used for packet forwarding. It does not affect the link state database, nor does it affect the

neighbor's routing table.

1.9.3 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
- Disabling Interfaces from Sending OSPF Packets
- Configuring Inter-area Route Filtering
- Configuring Redistributed Route Filtering
- Configuring Learned Route Filtering

1.9.4 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. A passive interface cannot send and receive OSPF packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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.

1.9.5 Disabling Interfaces from Sending OSPF Packets

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the function of filtering LSA update packets.

ip ospf database-filter all out

By default, the function of diffusing LSA packets to the outside is enabled on an interface, that is, any LSA update packet can be sent from the interface.

1.9.6 Configuring Inter-area Route Filtering

1. Overview

Route filtering can prevent routes from being added to routing table or advertised to neighbors. Users on the network will not access the specified destination network.

2. Restrictions and Guidelines

- This command can be configured only on an ABR.
- This command can be used when you need to configure filtering conditions for route learning between different areas on the ABR.
- This command is recommended when you need to prevent users from accessing 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 routing 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.

1.9.7 Configuring Redistributed Route Filtering

1. Overview

The redistributed route filtering function refers to filtering routes redistributed from other protocols to OSPF. The **distribute-list out** command is similar to the **redistribute route-map** command, but it 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(5) Configure redistributed route filtering.

distribute-list { [*acl-name* | *acl-number*] | **prefix** *prefix-list-name* } out [**arp-host** | **connected** | **ospf** *process-id* **| rip | static**]

By default, the filtering function of redistributed routes is disabled, that is, all the redistributed routes get past.

1.9.8 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.

  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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(5) Configure learned route filtering.

distribute-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*]

By default, the filtering function of the routes calculated based on the received LSA is disabled, that is, all these routes get passed.

1.10 Adjusting OSPF Network Convergence Speed

1.10.1 Overview

This function aims to modify protocol control parameters to change the protocol running status, thus adjusting the convergence speed of OSPF network.

1.10.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- The neighbor relationship maintenance time cannot be shorter than the hello interval.

1.10.3 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

1.10.4 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the hello interval.

ip ospf hello-interval *hello-interval*

By default, the hello packet interval is 10s for Ethernet 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.

1.10.5 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.
- 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

1.10.6 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure LSU transmission delay.

ip ospf transmit-delay *transmit-delay*

The LSU packet transmission delay is 1s by default.

1.10.7 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the LSU retransmission interval.

ip ospf retransmit-interval *retransmit-interval*

By default, the LSU retransmission interval is 5s.

1.10.8 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 *delay-time, hold-time* and *max-wait-time* 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 routing 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.

1.10.9 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 routing 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.

1.10.10 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 routing 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.

1.10.11 Configuring Duplicate LSA Receiving Delay

1. Overview

To prevent excessive usage of network bandwidth and device resources caused by frequent network connection or routing turbulence, you can configure the device to not process duplicate LSAs within a specified time according to the network connection and device resources in the current network.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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.

1.10.12 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 routing 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 calculation is 0 ms.

1.10.13 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 routing 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 calculation is 0 ms.

1.10.14 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, the **timers throttle spf** 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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the SPF computation delay. Select one of the following items to configure.

- **timers throttle spf** *spf-delay spf-holdtime spf-max-waittim*e

By default, the delay for SPF computation is 50 ms, the minimum interval for two SPF calculations is 200 ms, and the maximum interval between two SPF calculations is 5000 ms.

- **timers spf** *spf-delay spf-holdtime*

By default, the **timers spf** command does not take effect. The SPF calculation delay is subject to the default configuration of the **timers throttle spf** command.

1.10.15 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 routing 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.

1.11 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. If the same authentication type must be enabled on all interfaces in an area, you are advised to make the configuration through the area authentication type. If the router accesses the network that requires authentication, then area authentication or interface authentication must be configured.

2. Restrictions and Guidelines

- 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 authentication key must be configured using the **key chain** command. 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 OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the authentication type of an area.

area *area-id* **authentication** [**keychain** *keychain-name* | **message-digest**]

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. This configuration is mandatory if different authentication types are enabled on different interfaces in the same area. If the router accesses the network that requires authentication, then area authentication or interface authentication must be configured.

2. Restrictions and Guidelines

- If the **ip ospf authentication** command does not contain any option, plain text authentication is enabled. 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.
- If area authentication has been configured, the interface authentication mode is determined by the area authentication configuration when the **no** option is used to restore the interface authentication mode to the default value.

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 Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the authentication type of an interface.

ip ospf authentication [**keychain** *keychain-name* | **message-digest** | **null**]

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.
- The current OSPF version supports AES128 encryption and simple encryption. When encryption authentication is enabled globally, AES128 encryption algorithm is preferred for key encryption. The maximum length of AES128 encryption key is 21 characters, and the maximum length of simple encryption key is 18 characters. You are advised to configure the AES128 encryption key because the AES128 encryption is more secure.

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 Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure plain text authentication for an interface.

ip ospf authentication

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.

(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.
- The current OSPF version supports AES128 encryption and simple encryption. When encryption authentication is enabled globally, AES128 encryption algorithm is preferred for key encryption. The maximum length of AES128 encryption key is 21 characters, and the maximum length of simple encryption key is 18 characters. You are advised to configure the AES128 encryption key because the AES128 encryption is more secure.
- 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure cipher text authentication for an interface.

ip ospf authentication message-digest

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.

(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

After the fast reroute function is enabled, once OSPF detects a route failure, the router can immediately switch to the second-best route, helping 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

Fast reroute will prepare a backup route for OSPF. Once OSPF detects a neighbor failure, the router will immediately forward the traffic to the backup route to avoid traffic interruption. 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 routing 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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. If you do not want to forward the data traffic to the specified path after the optimal path fails, you must disable an interface as a backup interface for fast rerouting. When the optimal path fails, the traffic will switch to other suboptimal paths. After the OSPF protocol finally converges again, a new optimal path will be selected according to the interface cost.

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. If the remaining bandwidth of an interface is small or an interface may fail with the primary interface at the same time, the interface is not suitable as a backup interface. In this case, you need to disable the interface as a backup interface in the interface configuration mode of the interface. After an interface is disabled as a backup interface, the backup interface will be selected from other interfaces during OSPF fast rerouting calculation.
- 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Prevent an interface from becoming a backup interface.

ip ospf fast-reroute no-eligible-backup

By default, all interfaces can be used as a backup interface of OSPF fast reroute.

1.13 Modifying the Maximum Number of Concurrent Neighbors

1.13.1 Overview

Modifying the maximum number of concurrent neighbors 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 use this command to restrict the maximum of neighbors with which each OSPF process can concurrently initiate or accept interaction. 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.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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. 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.

2. 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.

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. When the topology detection function is enabled, the device can detect the topology changes during GR.

2. Restrictions and Guidelines

- You are advised to retain the default configuration.
- If the topology detection function is disabled, the topology change in the GR process cannot be converged in time, which may cause a long-time forwarding black hole.
- If the topology detection function is enabled, forwarding may be interrupted when the topology changes, but the interruption time is far shorter than that when the topology detection function is disabled.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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, GR Helper advertises a Grace-LSA to 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.

- The **disable** option indicates that the GR helper is not provided for any device that implements GR.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the OSPF 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 Correlating OSPF with BFD

1.15.1 Overview

After OSPF is correlated with BFD, 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 correlation with BFD is configured for both the OSPF 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Configure the association between OSPF interfaces and BFD.

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 routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enter the OSPF routing configuration mode and associate with BFD.

bfd all-interfaces

By default, the BFD function is disabled on all the interfaces.

1.16 Enabling Overflow

1.16.1 Overview

When the overflow function is enabled, 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 routing 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. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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 device enters the overflow state. In this state, the device no longer loads external LSAs and deletes external LSAs that are generated locally. After the configured waiting time elapses, the device restores the normal state, and loads external LSAs again.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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 Network Management Functions

1.17.1 Overview

Use the network management software to manage OSPF parameters and monitor the OSPF running status.

1.17.2 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.

1.17.3 Configuration Tasks

The configuration of network management functions includes the following tasks, which are optional. Select tasks for configuration according to actual condition.

- Binding the MIB with an OSPF Process
- Configuring the Trap Function
- Configuring the Logging Function

1.17.4 Binding the MIB with an OSPF Process

1. Overview

- 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 want to manage the parameters of a specified OSPFv2 process through network management software, you must bind the MIB to the OSPFv2 process.

2. Restrictions and Guidelines

- If you want 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 routing 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.

1.17.5 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 routing 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.

1.17.6 Configuring the Logging Function

1. Overview

The logging function can be enabled to record the change log of the adjacent state to facilitate the analysis and search of relevant information. By default, the logging function is enabled. 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.

2. Restrictions and Guidelines

You are advised to retain the default configuration. If you want to reduce the log output, disable this function.

- If the **detail** parameter is configured, the change log of all adjacent states will be recorded.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing 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.

1.18 Enabling NSR

1.18.1 Overview

If the NSR function is enabled, the device can maintain a stable adjacency state during the active/standby switchover, so as to ensure that data forwarding continues and is not interrupted.

1.18.2 Restrictions and Guidelines

- The OSPF basic functions must be configured.
- 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 active/standby switchover 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. If the fast hello function is enabled, the OSPF neighbor keepalive duration is less than 1s. therefore, you are advised to disable the fast hello function when the NSR function is enabled.

1.18.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Enable the NSR function.

nsr

The NSR function is disabled by default.

1.19 Enabling the iSPF Feature

1.19.1 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.

1.19.2 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.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure the **i**SPF feature.

ispf enable

The iSPF feature is disabled by default.

1.20 Configuring to Disable MTU Verification

1.20.1 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.

1.20.2 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.

1.20.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

interface loopback *interface-number*

(4) Configure to disable MTU verification.

ip ospf mtu-ignore

The MTU verification function is disabled by default.

1.21 Configuring to Enable Conflict Detection of Type-4 LSAs

1.21.1 Overview

This function enables conflict detection for received Type-4 LSAs.

1.21.2 Restrictions and Guidelines

The OSPF basic functions must be configured before using this function.

1.21.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPF routing configuration mode.

router ospf *process-id* [**vrf** *vrf-name*]

(4) Configure conflict detection of Type-4 LSAs.

detect-conflict lsa-4

Conflict detection for Type-4 LSAs 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, OSPF must run on a super VLAN, and the packets only need to be sent over a sub VLAN of the super VLAN. In this case, you can run the **ip ospf subvlan** command to specify a sub VLAN ID for sending packets, so as 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 SVI configuration mode.

interface vlan *interface-number*

(4) Enable OSPF for the super VLAN.

ip ospf subvlan [**all** | *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.

Command	Purpose
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** [**adv-router** *ipv4-address* | { **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** [*net-address/mask*] | **opaque-as** [*net-address/mask*] | **opaque-link** | **router** | **summary** } [*link-state-id* | **adv-router** *ipv4-address* | **brief** | **self-originate**] | **database-summary** | **detail** | **max-age** | **self-originate**]	Displays the information of the OSPF LSDB.
show ip ospf [*process-id*] **diagnosis auth-fails** [**interface** *interface-type interface-number*] [**with-clear**]	Displays statistics on OSPF packet diagnosis information.
show ip ospf [*process-id*] **flood** [**normal** | **realtime** | **statistics**]	Displays the LSA flooding information.
show ip ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]	Displays the OSPF-enabled interface.
show ip ospf [*process-id*] **ispf**	Displays the number of times a route is computed in the OSPF area through iSPF.
show ip ospf [*process-id*] **neighbor** [{ *interface-type interface-number* | *neighbor-id* | **detail** } * | **last-down** | **statistics**]	Displays the neighbor list of an OSPF process.
show ip ospf [*process-id*] **redist-info** [**global**]	Displays OSPF redistribution information.
show ip ospf route record	Displays OSPF route distribution records.
show ip ospf [*process-id*] **route** [**count** | *ipv4-address mask*]	Displays the OSPF routing table.
show ip ospf [*process-id*] **spf**	Displays the number of times SPT is computed in the OSPF area.
show ip ospf [*process-id*] **statistics**	Displays OSPF statistics.
show ip ospf [*process-id*] **summary-address**	Displays the summarized route of OSPF redistributed routes.

Command	Purpose
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** [*ipv4-address*]	Displays OSPF virtual links.
show running-config router ospf	Displays the OSPF configuration.
clear ip ospf [*process-id*] **ase**	Clears and recalculates OSPF external routes.
clear ip ospf [*process-id*] **process**	Clears and resets an OSPF process.
clear ip ospf [*process-id*] **redistribution**	Clears and redistributes OSPF routes.
clear ip ospf [*process-id*] **spf**	Clears and recalculates the SPF calculation result of OSPF.
clear ip ospf thread-list	Clears the pseudo-thread list of the 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

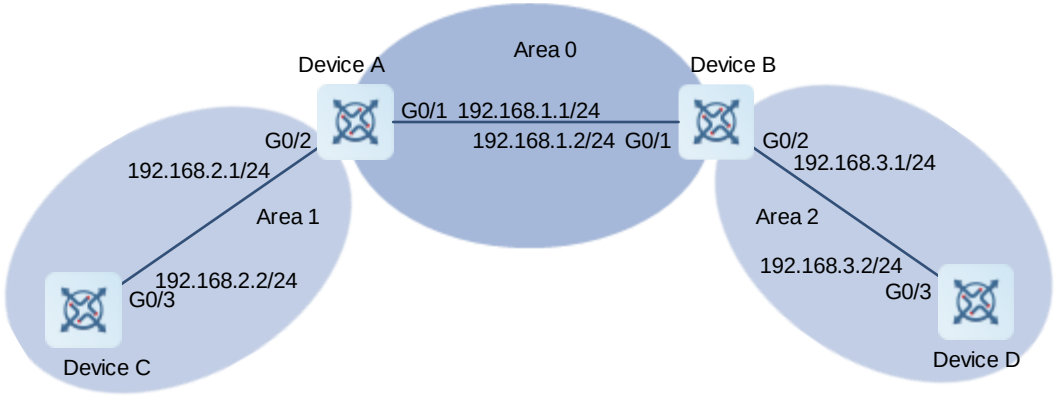
1.24.1 Configuring Basic Functions of OSPF

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 1-10 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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
```

```
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# no switchport
DeviceA(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# no switchport
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# no switchport
DeviceB(config-if-GigabitEthernet 0/2)# ip address 192.168.3.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface gigabitethernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# no switchport
DeviceC(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/3)# exit
```

Configure Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# interface gigabitethernet 0/3
DeviceD(config-if-GigabitEthernet 0/3)# no switchport
DeviceD(config-if-GigabitEthernet 0/3)# ip address 192.168.3.2 255.255.255.0
DeviceD(config-if-GigabitEthernet 0/3)# exit
```

(2) Configure the OSPF process, router ID, and add the interface IP address to the OSPF process.

Configure Device A.

```
DeviceA(config)# router ospf 1
DeviceA(config-router)# router-id 192.168.1.1
DeviceA(config-router)# network 192.168.1.0 0.0.0.255 area 0
DeviceA(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

Configure Device B.

```
DeviceB(config)# router ospf 1
DeviceB(config-router)# router-id 192.168.1.2
DeviceB(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

```
DeviceB(config-router)# network 192.168.3.0 0.0.0.255 area 2
```

Configure Device C.

```
DeviceC(config)# router ospf 1
DeviceC(config-router)# router-id 192.168.2.2
DeviceC(config-router)# network 192.168.2.0 0.0.0.255 area 1
```

Configure Device D.

```
DeviceD(config)# router ospf 1
DeviceD(config-router)# router-id 192.168.3.2
DeviceD(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.

```
DeviceA# 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.

```
DeviceA# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State       BFD 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.

```
DeviceB# show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.1, 00:18:03, GigabitEthernet 0/1
```

Check the neighbor information of Device B.

```
DeviceB# show ip ospf neighbor
OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID   Pri   State       BFD 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.

```
DeviceC# 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.

```
DeviceC# 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    -         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.

```
DeviceD# 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.

```
DeviceD# 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    -         00:00:30    192.168.3.1   GigabitEthernet
0/3
```

(5) Ping 192.168.2.2 on Device D. The network is reachable.

```
DeviceD# 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
 no switchport
 ip address 192.168.1.1 255.255.255.0
!
interface gigabitethernet 0/2
 no switchport
 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
 no switchport
 ip address 192.168.1.2 255.255.255.0
!
interface gigabitethernet 0/2
 no switchport
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
 no switchport
 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
 no switchport
 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

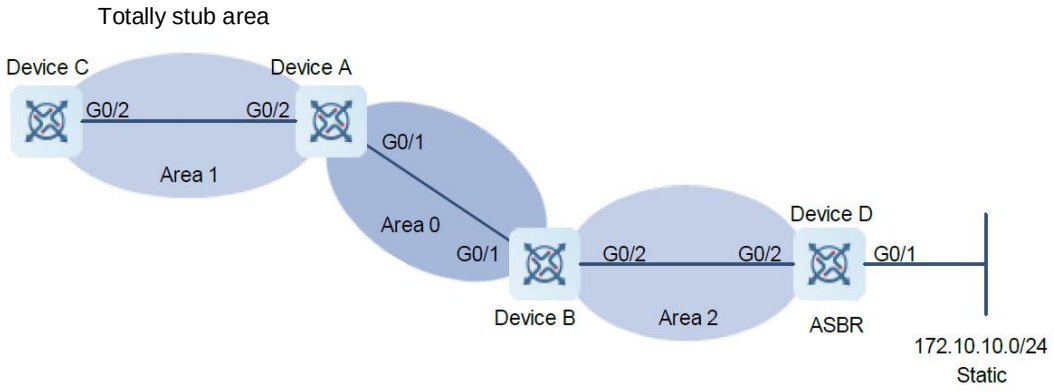
Device A, Device B, Device C, and Device D are interconnected through the OSPF routing protocol.

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 1-11 Topology for a Stub Area



3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Configure Area 1 as a stub area on Device A and Device C.

4. Procedure

(1) Introduce an external static route to Device D.

```
DeviceD> enable
DeviceD# configure terminal
```

```
DeviceD(config)# router ospf 1
DeviceD(config-router)# redistribute static subnets
```

(2) Configure Area 1 as a stub area on Device A and Device C.

Configure Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# router ospf 1
DeviceA(config-router)# area 1 stub no-summary
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# router ospf 1
DeviceC(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.

```
DeviceC# show ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2
```

On Device A, run the **show ip route ospf** command to display the routing table. Verify that external static routes are introduced from Device D.

```
Device A# show ip route ospf
O E2  172.10.10.0/24 [110/20] via 192.168.1.2, 00:01:59, GigabitEthernet 0/1
O IA  192.168.3.0/24 [110/2] via 192.168.1.2, 00:41:01, GigabitEthernet 0/1
```

On Device B, run the **show ip route ospf** command to display the routing table. Verify that external static routes are introduced from Device D.

```
Device B# show ip route ospf
O E2  172.10.10.0/24 [110/20] via 192.168.3.2, 00:02:53, GigabitEthernet 0/2
O IA  192.168.2.0/24 [110/2] via 192.168.1.1, 00:42:02, GigabitEthernet 0/1
```

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, and Device C are interconnected through the OSPF routing protocol.

Device B, as an ABR, is responsible for the routing information transfer between OSPF areas, and Device C functions as an ASBR to import the external static route.

To reduce the number of LSAs in Area 1 and save the device performance, Area 1 is configured as an NSSA.

2. Topology

Figure 1-12 Topology for an NSSA

3. Notes

- Configure interface IP addresses for all devices (omitted).
- Configure OSPF basic functions on all devices (omitted).
- Device C needs to import an external static route to the OSPF process.
- Configure Area 1 as NSSA on Device B and Device C.

4. Procedure

(1) Configure a static route for Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.2
```

(2) Introduce an external static route to Device C.

```
DeviceC(config)# router ospf 1
DeviceC(config-router)# redistribute static subnets
```

(3) Configure Area 1 as NSSA on Device B and Device C.

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# router ospf 1
DeviceB(config-router)# area 1 nssa
```

Configure Device C.

```
DeviceC(config-router)# area 2 nssa
```

5. Verification

On Device C, check the Type-7 LSAs generated from 172.10.10.0/24.

```
DeviceD# 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.

```
DeviceB# 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.

```
DeviceB# 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 1 nssa
!
```

- Device C configuration file

```
!
ip route 172.10.10.0 255.255.255.0 192.168.6.2
!
router ospf 1
 redistribute static subnets
 area 1 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

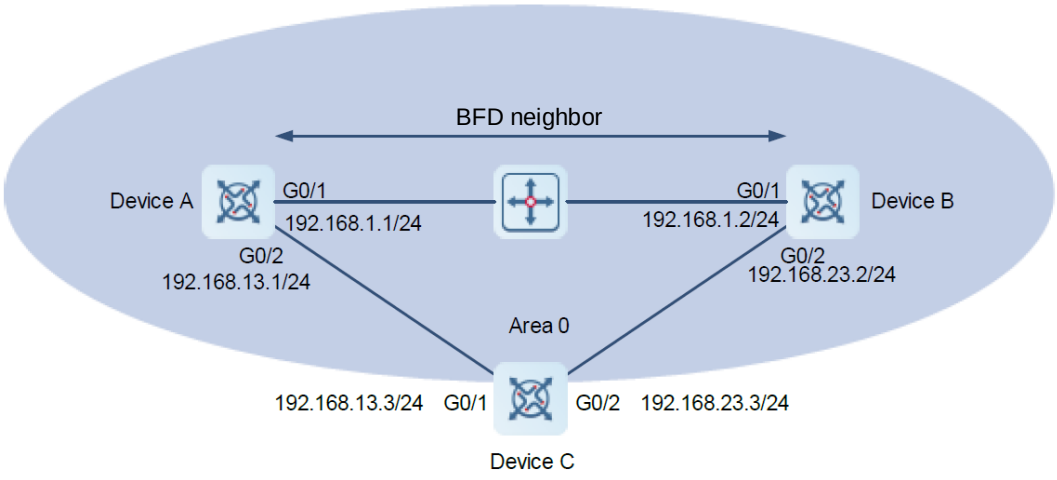
1. Requirements

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 1-13 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 Device A and Device B.
- Correlate OSPF with BFD on Device A and Device B.

4. Procedure

(1) Configure BFD parameters for the interfaces of Device A and Device B.

Configure Device A.

```
DeviceA> enable
DeviceA# configure terminal
```

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

(2) Correlate OSPF with BFD on Device A and Device B.

Configure Device A.

```
DeviceA(config)# router ospf 1
DeviceA(config-router)# bfd all-interfaces
```

Configure Device B.

```
DeviceB(config)# router ospf 1
DeviceB(config-router)# bfd all-interfaces
```

5. Verification

On Device A, verify that correlating OSPF with BFD is up.

```
DeviceA# 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     Admin     00:00:40   192.168.13.3
GigabitEthernet 0/2
```

On Device B, verify that correlating OSPF with BFD is up.

```
DeviceB# 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     Admin     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
```

```
!
router ospf 1
 bfd all-interfaces
!
```

- Device B configuration file

```
!
interface gigabitethernet 0/1
 bfd interval 200 min_rx 200 multiplier 5
!
router ospf 1
 bfd all-interfaces
!
```

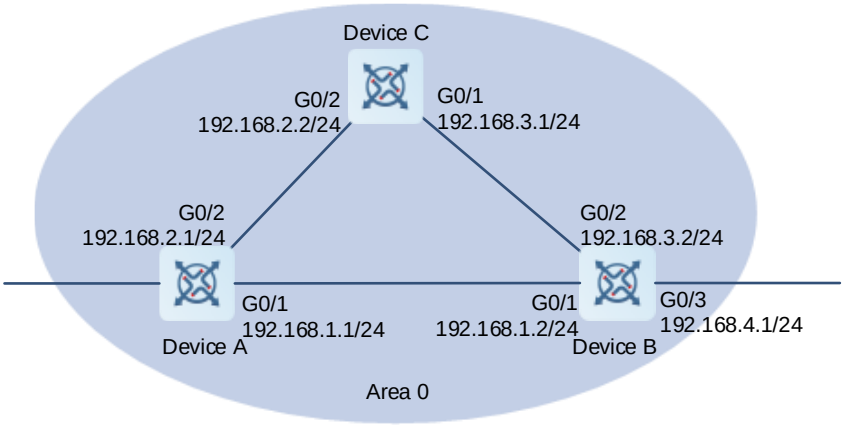
1.24.5 Configuring Fast Reroute

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 1-14 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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# router ospf 1
DeviceA(config-router)# fast-reroute lfa
DeviceA(config-router)# exit
```

(4) Configure carrier-delay 0 on all the interfaces of Device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# carrier-delay 0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(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.

```
DeviceA# 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
!
```

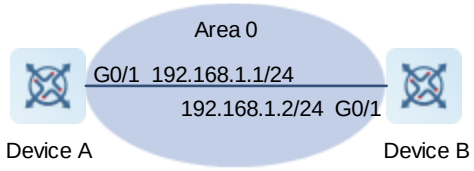
1.24.6 Configuring Network Management Functions

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 1-15 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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# snmp-server host 192.168.2.2 traps version 2c public
DeviceA(config)# snmp-server community public rw
DeviceA(config)# snmp-server enable traps
```

(4) Configure the trap function in OSPF process 10.

```
DeviceA(config)# router ospf 10
DeviceA(config-router)# enable mib-binding
DeviceA(config-router)# enable traps
```

5. Verification

Verify the SNMP information before the trap function is configured for the OSPF process.

```
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: disable
SNMP logging: disabled
SNMP trap logging: disabled
SNMP authentication success logging: enabled
SNMP authentication fail logging: enabled
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.

```
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
   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
```

```
SNMP global trap: enabled
SNMP logging: disabled
SNMP trap logging: disabled
SNMP authentication success logging: enabled
SNMP authentication fail logging: enabled
SNMP agent: enabled
SNMP v1:  enabled
SNMP v2c: enabled
SNMP v3:  enabled
```

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.

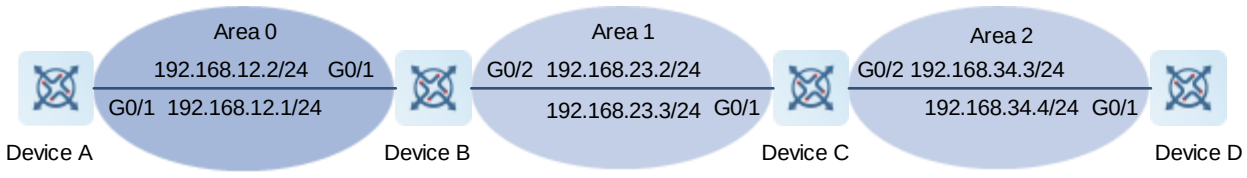
1.24.7 Configuring a Virtual Link

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 1-16 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. Set router IDs of Devices A to D to 192.168.12.1, 192.168.12.2, 192.168.23.3, and 192.168.34.4, respectively (omitted).

(2) Configure a virtual link on Devices B and C.

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# router ospf 1
DeviceB(config-router)# area 1 virtual-link 192.168.23.3
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# router ospf 1
DeviceC(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.

```
DeviceA# show ip ospf database
          OSPF Router with ID (192.168.12.1) (Process ID 1)
              Router Link States (Area 0.0.0.0)
Link ID        ADV Router     Age        Seq#      CKSum   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          0x80000001 0x001328 0
              Network Link States (Area 0.0.0.0)
Link ID        ADV Router     Age        Seq#      CKSum
192.168.12.1   192.168.12.1   1031       0x80000001 0x00CE8E
              Summary Link States (Area 0.0.0.0)
Link ID        ADV Router     Age        Seq#      CKSum      Route
192.168.23.0   192.168.12.2   820        0x80000001 0x0077CC   192.168.23.0/24
192.168.23.0   192.168.23.3   7          0x80000001 0x002414   192.168.23.0/24
192.168.34.0   192.168.23.3   7          0x80000001 0x00AA82   192.168.34.0/24
```

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
!
```

1.24.8 Selecting a DR of OSPF

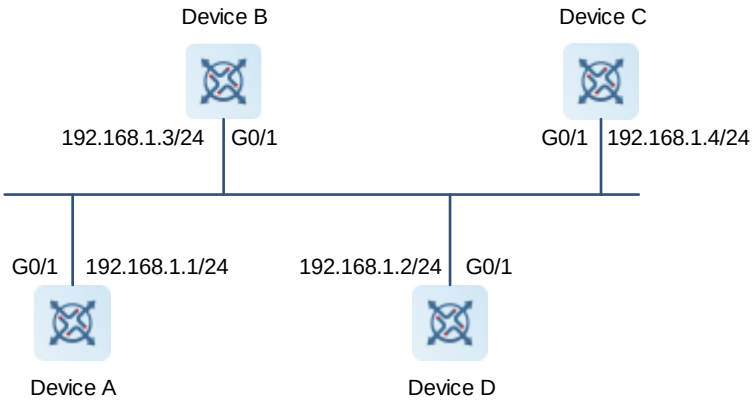
1. Requirements

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 1-17 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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip ospf priority 10
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip ospf priority 5
```

Configure Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# interface gigabitethernet 0/1
DeviceD(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.

```
DeviceD# 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
192.168.1.3      5    FULL/BDR        00:00:30    192.168.1.3    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 20
1.3.4 Configuring OSPFv3 20
1.3.5 Creating a Virtual Link 21
1.4 Configuring OSPFv3 Network Types 22
1.4.1 Overview 22
1.4.2 Restrictions and Guidelines 22
1.4.3 Prerequisites 22
1.4.4 Procedure 22
1.5 Configuring OSPFv3 Route Advertisement 23
1.5.1 Overview 23
1.5.2 Configuration Tasks 23
1.5.3 Configuring External Route Redistribution 23

1.5.4 Generating a Default Route 24
1.5.5 Configuring a Device as ASBR 25
1.6 Configuring Stub Area and NSSA 25
1.6.1 Overview 25
1.6.2 Restrictions and Guidelines 25
1.6.3 Prerequisites 26
1.6.4 Procedure 26
1.7 Configuring OSPFv3 Route Summarization 26
1.7.1 Overview 26
1.7.2 Restrictions and Guidelines 26
1.7.3 Prerequisites 27
1.7.4 Procedure 27
1.8 Configuring OSPFv3 Route Filtering 27
1.8.1 Overview 27
1.8.2 Restrictions and Guidelines 27
1.8.3 Prerequisites 28
1.8.4 Procedure 28
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 Configuration Tasks 29
1.9.5 Configuring Reference Bandwidth 29
1.9.6 Configuring Interface Cost 29

1.9.7 Configuring Cost Value of Default Route in Stub Area or NSSA 30
1.9.8 Configuring Default Metric of Redistributed Routes 31
1.9.9 Configuring Administrative Distance 32
1.10 Adjusting OSPFv3 Network Convergence Speed 32
1.10.1 Overview 32
1.10.2 Prerequisites 32
1.10.3 Configuration Tasks 32
1.10.4 Configuring Transmission Time of OSPFv3 Packets 33
1.10.5 Configuring OSPFv3 Route Computation Time 34
1.11 Enabling OSPFv3 Authentication 36
1.11.1 Overview 36
1.11.2 Restrictions and Guidelines 36
1.11.3 Prerequisites 36
1.11.4 Configuration Tasks 36
1.11.5 Configuring Instance Authentication and Encryption 36
1.11.6 Configuring Area Authentication and Encryption 37
1.11.7 Configuring Interface Authentication and Encryption 38
1.12 Enabling Two-Way Maintenance 39
1.12.1 Overview 39
1.12.2 Prerequisites 39
1.12.3 Procedure 40
1.13 Correlating OSPFv3 with BFD 40
1.13.1 Overview 40
1.13.2 Restrictions and Guidelines 40

1.13.3 Prerequisites 40
1.13.4 Configuration Tasks 40
1.13.5 Correlating OSPFv3 and BFD on an Interface 40
1.13.6 Correlating OSPFv3 and BFD Globally 41
1.14 Enabling the GR Function 42
1.14.1 Overview 42
1.14.2 Restrictions and Guidelines 42
1.14.3 Prerequisites 42
1.14.4 Procedure 42
1.15 Enabling NSR 43
1.15.1 Overview 43
1.15.2 Restrictions and Guidelines 43
1.15.3 Prerequisites 43
1.15.4 Procedure 43
1.16 Enabling Conflict Detection of Type 4 LSAs 43
1.16.1 Overview 43
1.16.2 Prerequisites 43
1.16.3 Procedure 44
1.17 Modifying the Maximum Number of Concurrent Neighbors 44
1.17.1 Overview 44
1.17.2 Procedure 44
1.18 Configuring Network Management Functions 44
1.18.1 Overview 44
1.18.2 Restrictions and Guidelines 45

1.18.3 Prerequisites 45
1.18.4 Procedure 45
1.19 Disabling MTU Verification 45
1.19.1 Overview 45
1.19.2 Prerequisites 46
1.19.3 Procedure 46
1.20 Enabling OSPFv3 on a Super VLAN 46
1.20.1 Overview 46
1.20.2 Restrictions and Guidelines 46
1.20.3 Prerequisites 46
1.20.4 Procedure 47
1.21 Monitoring 47
1.22 Configuration Examples 49
1.22.1 Configuring Basic Functions of OSPFv3 49
1.22.2 Configuring OSPFv3 Authentication 55
1.22.3 Configuring a Stub Area 56
1.22.4 Configuring an NSSA 58
1.22.5 Selecting an OSPFv3 DR 61
1.22.6 Configuring BFD for OSPFv3 64
1.22.7 Configuring OSPFv3 Route Summarization 69

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.

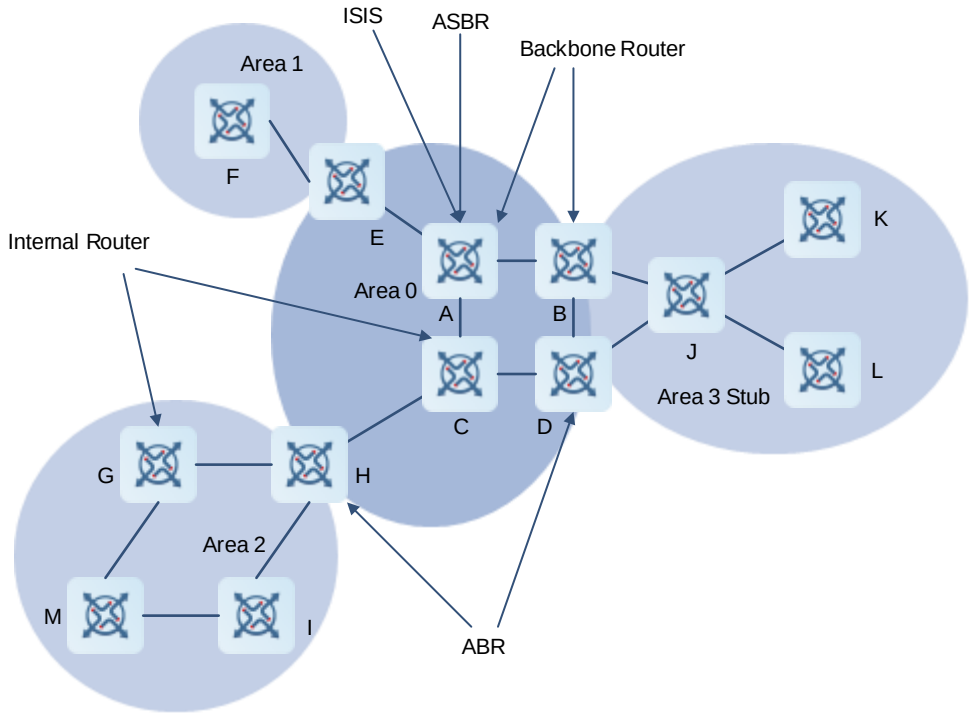
⚠ Caution

- 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.

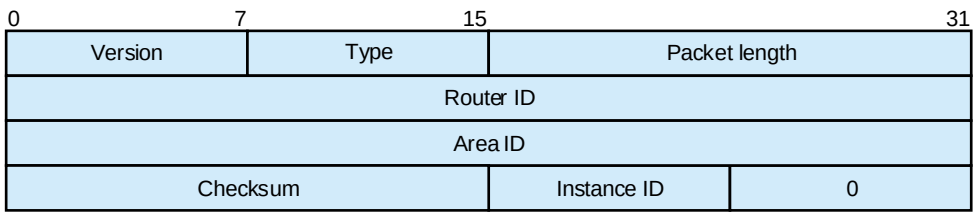
Note

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.

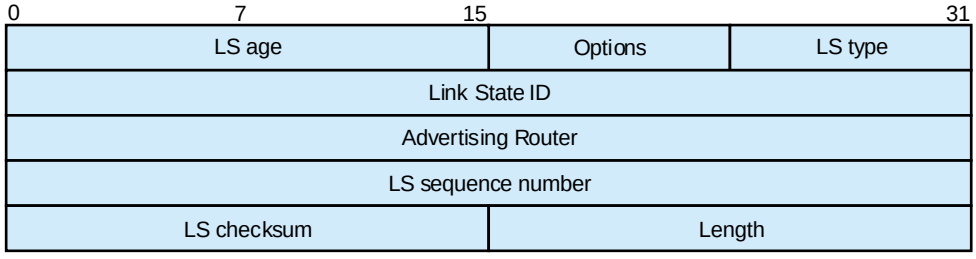
Table 1-1 Types of OSPFv3 Packets

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 x (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

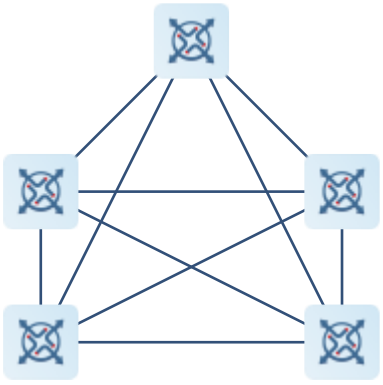
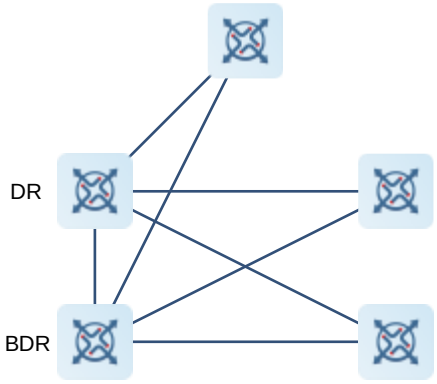


Figure 1-5 Number of Adjacency Relationships After DR Election

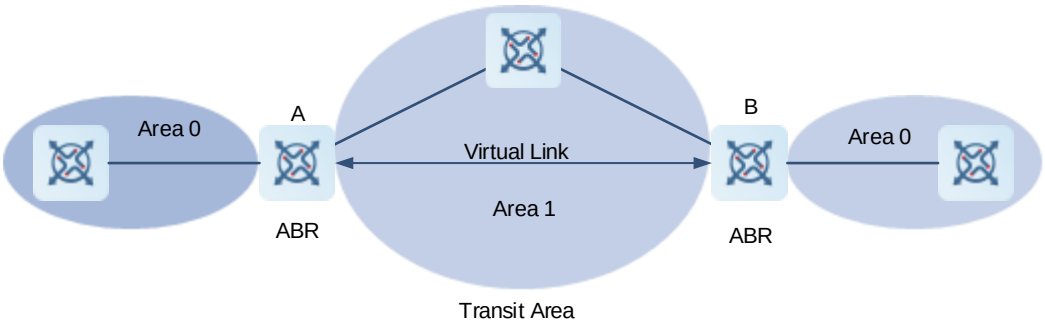


12. Virtual link

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.

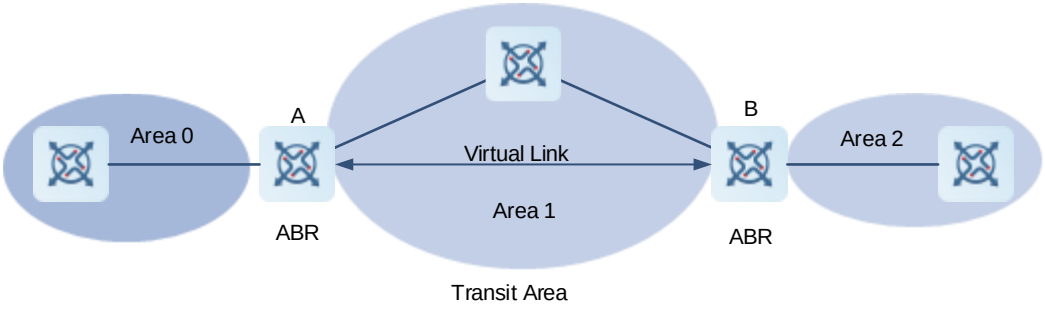
A virtual link relies on an OSPFv3 intra-domain route, making two ABRs adjacent. The OSPFv3 packet information exchanged by ABRs is transparent to the intermediate device.

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

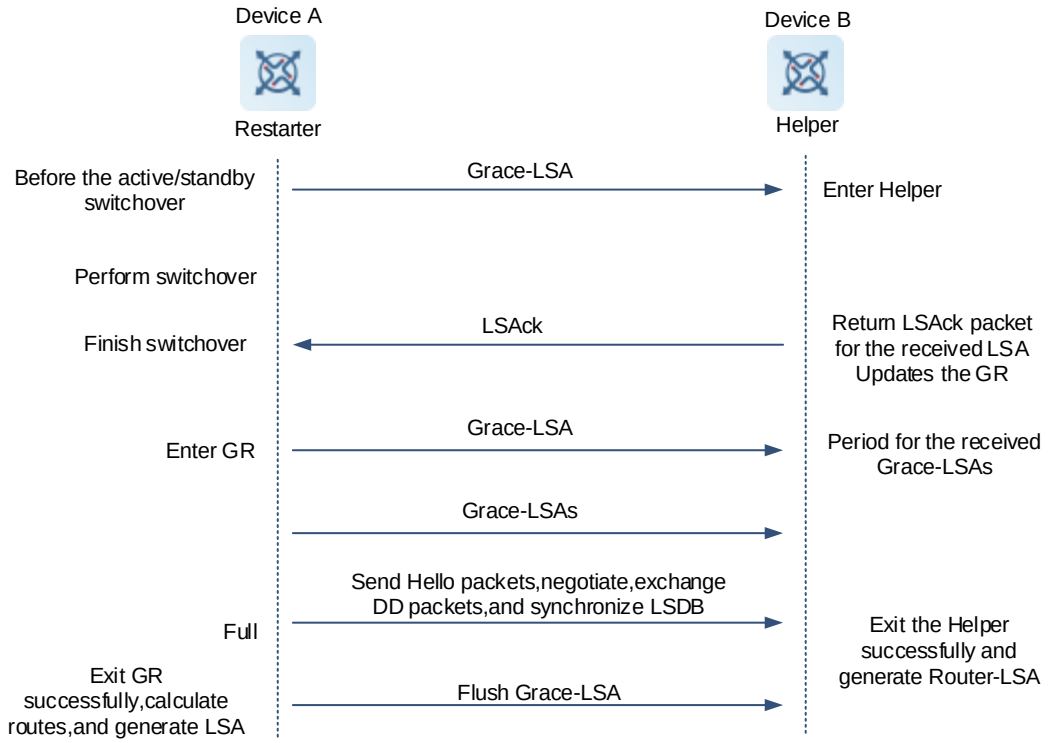
  When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPFv3 process is restricted, the router can interact with neighbors by batches, which ensures data forwarding 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, OSPFv3 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. The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Reference Bandwidth
- Configuring Interface Cost
- Configuring Default Metric of Redistributed Routes
- Configuring Administrative Distance

(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 Instance Authentication and Encryption
- Configuring Area Authentication and Encryption
- Configuring Interface Authentication and Encryption

(10) (Optional) Enabling Two-Way Maintenance

(11) (Optional) Correlating OSPFv3 with BFD. The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Correlating OSPFv3 and BFD on an Interface
- Correlating OSPFv3 and BFD Globally

(12) (Optional) Enabling the GR Function

(13) (Optional) Enabling NSR

(14) (Optional) Enabling Conflict Detection of Type 4 LSAs

(15) (Optional) Modifying the Maximum Number of Concurrent Neighbors

(16) (Optional) Configuring Network Management Functions

(17) (Optional) Disabling MTU Verification

(18) (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.
- An OSPFv3 process can be configured with a maximum of 1,000 non-backbone areas.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an OSPFv3 process and enter the OSPFv3 routing 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) (Optional) Configure a specified OSPFv3 area.

area area-id

No OSPFv3 area is configured by default.

(6) Return to the global configuration mode.

exit

(7) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 aggregated interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(8) 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.
- To modify the key corresponding to the security parameter index (SPI) configured for the specified virtual link, run the **no area virtual-link authentication** or **no area virtual-link encryption** command based on configurations. You can reconfigure the key only after deleting authentication configuration.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing 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* | **ipsec sa** *sa-name* | **retransmit-interval** *retransmit-interval* | **transmit-delay** *transmit-delay*] * [**authentication ipsec spi** *spi* { **md5** | **sha1 | sha2-256** } [**0** | **7**] *key* | **encryption ipsec spi** *spi* **esp** [**3des** | **aes-cbc** { **128** | **192** | **256** } [**0** | **7**] *des-key* | **des** [**0** | **7**] *des-key* | **null**] { **md5** | **sha1** } [**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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregated interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure external route redistribution.

redistribute { **connected** | **ospf** *process-id* [**match** { **externa**l [**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**.

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 routing 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.

2. 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing 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 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** | **translate type7 suppress-fa** | **translator** { **always** | **stability-interval** *stability-interval* } * | **zero-address-forwarding**] *

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 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 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** [**connected** | **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* | **route-map** *route-map-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.

- Configure the interface cost.
- Configure cost of the default route in a stub area or an NSSA.
- Configure redistributed route cost.

- Modify the administrative distance.

1.9.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.9.4 Configuration Tasks

The configuration tasks for adjusting OSPF routing are as follows. The following configuration tasks are optional. Select tasks for configuration according to the actual condition.

- Configuring Reference Bandwidth
- Configuring Interface Cost
- Configuring Cost Value of Default Route in Stub Area or NSSA
- Configuring Default Metric of Redistributed Routes
- Configuring Administrative Distance

1.9.5 Configuring Reference Bandwidth

1. Overview

The default value of OSPFv3 reference bandwidth is 100 Mbps, and the cost is the reference bandwidth/actual bandwidth. In gigabit and 10-gigabit network environments, the calculated cost is 1. The default bandwidth cannot meet the requirements of today's high-speed transmission networks. The router connects routes of different bandwidths. You are advised to adjust the configuration according to the actual bandwidth if you want to give priority to lines with large bandwidth.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) 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.

1.9.6 Configuring Interface Cost

1. Overview

You can modify the interface cost of OSPFv3 to optimize routing. The lower the link cost, the higher the priority in routing.

2. Restrictions and Guidelines

- By default, the OSPFv3 interface cost is equal to the automatic cost reference value/interface bandwidth.
- A router connects multiple lines. You are advised to configure this function if you want to manually specify the priority route.
- You can use the **auto-post** command to configure the automatic reference cost. The default value is 100 Mbps.
- You can use the **bandwidth** command to configure the interface bandwidth.
- Default OSPF interface costs of typical lines:
  - For the 64K serial line, the cost is 1562;
  - For the E1 line, the cost is 48;
  - For the 10 Mbps Ethernet line, the cost is 10;
  - For the 100 Mbps Ethernet line, the cost is 1.
- If you have configured the interface cost using the **ipv6 ospf cost** command, the cost calculated automatically will be overwritten by the configured cost.

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 Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) 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.

1.9.7 Configuring Cost Value of Default Route in Stub Area or NSSA

1. Overview

After an area is configured as a Stub/NSSA area, the ABR will advertise the default route to the Stub/NSSA area to ensure that the route from the Stub/NSSA area to other areas is reachable. The default cost of the default

route is 1. If you want to reduce the routing priority of the default route, you can configure a higher cost for the default route.

2. Restrictions and Guidelines

The configuration can only take effect on the ABR of the Stub area or the ABR/ASBR of the NSSA area.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure the cost of the default route of the Stub/NSSA area.

area *area-id* **default-cost** *cost*

By default, the cost of the default route is 1.

1.9.8 Configuring Default Metric of Redistributed Routes

1. Overview

In the case of redistributing an external route, the cost of the external route can be flexibly adjusted for routing.

2. Restrictions and Guidelines

- This function must be configured when an external route is imported on the ASBR, in order to specify the cost of the external route.
- The **default-metric** command must be used with the **redistribute** routing configuration command to modify the initial metrics of all redistributed routes.
- The **default-metric** command does not take effect on external routes that are injected into the OSPFv3 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 OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Configure default metric of redistributed routes.

default-metric *metric*

By default, the metric for redistributed routes is 20.

1.9.9 Configuring Administrative Distance

1. Overview

Administrative distance can be used to select the best route when multiple routing protocols are used to reach the same destination. Administrative distance defines the reliability of a routing protocol. The lower the administrative distance, the higher the reliability, and the higher the priority of routing. The default administrative distance of OSPFv3 intra-domain routing, inter-domain routing and external routing is 110. You can set different administrative distances to control routing.

2. Restrictions and Guidelines

- This function must be configured if multiple unicast routing protocols run on the router at the same time, and you want to change the priority of OSPFv3 routing.
- You can use this command to specify different administrative distances for different OSPF routes.
- The lower the value of administrative distance, the higher the routing priority. If the value of administrative distance is 255, the routing table entry is not trusted and will not participate in packet forwarding.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) 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**.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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 routing 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 **50** ms, the minimum interval between two SPF computations is **200** ms, and the maximum interval between two SPF computations is **5000** 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 an OSPFv3 instance is associated with SA authentication, SA authentication takes effect on all the interfaces under this OSPFv3 instance.
- 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.
- Area authentication and area associated SA authentication are mutually exclusive, and interface authentication and interface associated SA authentication are mutually exclusive.

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 Instance Authentication and Encryption
- Configuring Area Authentication and Encryption
- Configuring Interface Authentication and Encryption

1.11.5 Configuring Instance Authentication and Encryption

1. Overview

Security association (SA) defines a set of security algorithms and keys to ensure IP security. If a service is associated with IPsec SA authentication, OSPFv3 uses an SA authentication key to authenticate and encrypt packets. After this function is enabled, SA authentication takes effect in all areas and on all interfaces.

2. Restrictions and Guidelines

- SA authentication can be removed from an interface by configuring **ipv6 ospf ipsec sa disable**.
- Authentication priorities of OSPFv3 instances, areas, and interfaces are arranged in an ascending order as follows: OSPFv3 SA authentication < area authentication < interface authentication.

3. Prerequisites

SA authentication is configured on IPsec.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) (Optional) Associate OSPFv3 routing processes with SA authentication.

ipsec sa *sa-name*

No OSPFv3 routing process is associated with SA authentication by default.

1.11.6 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 four authentication types:
  - No authentication (when authentication is not configured)
  - MD5
  - SHA1
  - SHA2-256
- 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.
- To modify the key corresponding to the SPI configured for the specified area, run the **no area authentication** or **no area encryption** command based on configurations. You can reconfigure the key only

after deleting authentication configuration.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing 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** | **sha2-256** } [**0** | **7**] *key*

The OSPFv3 area authentication function is disabled by default.

(5) (Optional) Configure area SA authentication.

area *area-id* **ipsec sa** *sa-name*

No OSPFv3 area is associated with SA authentication by default.

(6) (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.

1.11.7 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 four authentication types:
  - No authentication (when authentication is not configured)
  - MD5
  - SHA1
  - SHA2-256
- The device supports three encryption types:
  - DES
  - 3DES
  - AES-CBC
- The OSPFv3 encryption and authentication parameters configured on interfaces must be consistent.
- To modify the key corresponding to the SPI configured for an interface, run the **no ipv6 ospf authentication** or **no ipv6 ospf encryption** command based on configurations. You can reconfigure the key only after

deleting authentication configuration.

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 Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) (Optional) Configure interface authentication.

ipv6 ospf authentication { **ipsec spi** *spi* { **md5** [**string**-**key**] | **sha1** | **sha2-256** } [**0** | **7**] *key* } [**instance** *instance-id*]

By default, no authentication mode is configured on an interface. In this case, the authentication type of the related area is used on the interface.

(5) (Optional) Configure interface SA authentication.

ipv6 ospf ipsec sa { disable | *sa-name* **}** [**instance** *instance-id*]

No interface is associated with SA authentication by default.

(6) (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 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 OSPFv3 basic functions must be configured before this function is used.

1.13.4 Configuration Tasks

Correlating OSPFv3 with BFD includes the following configuration tasks. These configuration tasks are optional and can be configured according to the actual situation.

- Correlating OSPFv3 and BFD on an Interface
- Correlating OSPFv3 and BFD Globally

1.13.5 Correlating OSPFv3 and BFD on an Interface

1. Overview

You can configure to correlate OSPFv3 and BFD on a specified interface to quickly detect errors on the interface and to accelerate OSPFv3 convergence.

2. Restrictions and Guidelines

- The priority of BFD on an interface is higher than that of BFD in OSPFv3 routing process.

You can use the **ipv6 ospf bfd** command to select the specified interface to use BFD for link detection according to the actual environment, or use the **bfd all-interfaces** command in the OSPFv3 routing configuration mode to configure all interfaces participating in OSPF operation to use BFD for link detection, and use the **ipv6 ospf bfd disable** command to disable the BFD detection function on the specified interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

a Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

b Enable BFD on OSPFv3 interfaces.

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 routing configuration mode.

1.13.6 Correlating OSPFv3 and BFD Globally

1. Overview

OSPFv3 protocol dynamically discovers neighbors through Hello packet. When OSPFv3 enables the BFD detection function, BFD sessions will be established for neighbors that reach Full relationship, and detect neighbor status through BFD mechanism. Once a BFD neighbor fails, OSPFv3 will immediately conduct network convergence.

2. Restrictions and Guidelines

You can use the **ipv6 ospf bfd** [**disable**] command in the interface configuration mode to enable or disable the BFD function on the specified interface. The priority of BFD function configured in interface configuration mode is higher than that of the BFD function configured using **bfd all-interfaces** command on all interfaces in the routing configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Enable BFD on all interfaces in the OSPFv3 process.

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 routing 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 routing 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 Enabling Conflict Detection of Type 4 LSAs

1.16.1 Overview

This function enables conflict detection for received Type 4 LSAs.

1.16.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing configuration mode.

ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

(4) Enable conflict detection of Type 4 LSAs.

detect-conflict lsa-4

Conflict detection for Type 4 LSAs is disabled by default.

1.17 Modifying the Maximum Number of Concurrent Neighbors

1.17.1 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.

1.17.2 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 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**.

1.18 Configuring Network Management Functions

1.18.1 Overview

Use the network management software to manage OSPFv3 parameters and monitor the OSPFv3 running status.

1.18.2 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.

1.18.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.18.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the OSPFv3 routing 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.

1.19 Disabling MTU Verification

1.19.1 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.

1.19.2 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.19.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.
- **interface** *ethernet-type interface-number*
- Enter the Layer 3 link aggregation configuration mode.
- **interface aggregateport** *interface-number*
- Enter the SVI configuration mode.
- **interface vlan** *interface-number*
- Enter the loopback interface configuration mode.
- **interface loopback** *interface-number*

(4) Disable MTU verification.

ipv6 ospf mtu-ignore

The MTU verification function is disabled by default.

1.20 Enabling OSPFv3 on a Super VLAN

1.20.1 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.

1.20.2 Restrictions and Guidelines

- The specified sub VLAN must be connected to neighbors.

1.20.3 Prerequisites

The basic OSPFv3 functions must be configured before this function is used.

1.20.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the SVI configuration mode.

interface *vlan interface-number*

(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.

1.21 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*] **flood** [**normal** | **realtime** | **statistics**]	Displays the LSA flooding information.
show ipv6 ospf [*process-id*] **interface** [*interface-type interface-number* | **brief**]	Displays the OSPFv3 interface.

Command	Purpose
show ipv6 ospf [*process-id*] **keepalive** [**area** [*area-id*] | **interface** [*interface-type interface-number*] [**with-clear** | **nbr**] | **process** | [**recv-queue** | **send-queue** | **virtual-link**] [**with-clear**]]	Displays OSPFv3 keepalive process information.
show ipv6 ospf [*process-id*] **neighbor** [*interface-type interface-number* [**detail**] | *neighbor-id* | **detail** | **last-down** | **statistics**]	Displays the neighbor list of OSPFv3.
show ipv6 ospf [*process-id*] **route** [**count**]	Displays the OSPFv3 routing table.
show ipv6 ospf route record	Displays OSPFv3 route distribution records.
show ipv6 ospf [*process-id*] **statistics**	Displays statistics on OSPFv3 route calculation.
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*] **ase**	Clears and recalculates OSPFv3 external routes.
clear ipv6 ospf [*process-id*] **process**	Clears and resets the OSPFv3 process.
clear ipv6 ospf [*process-id*] **redistribution**	Clears and redistributes OSPFv3 routes.
clear ipv6 ospf [*process-id*] **spf**	Clears and recalculates the SPF calculation result of OSPFv3.
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.

1.22 Configuration Examples

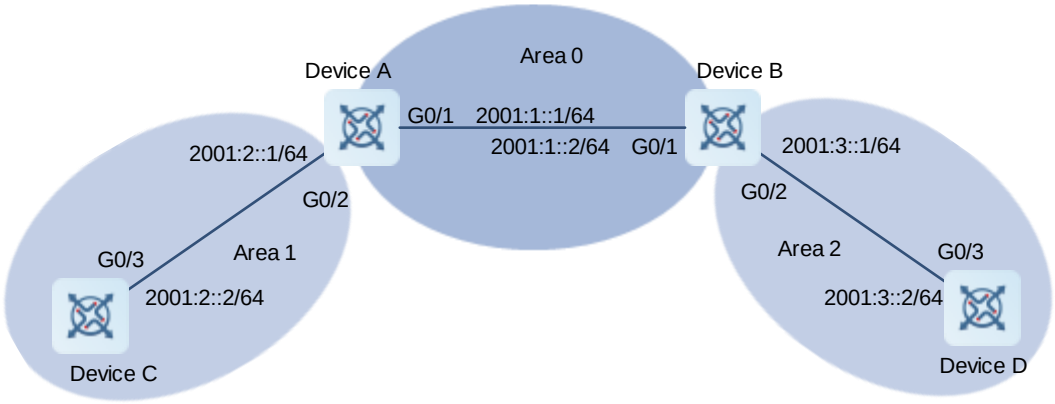
1.22.1 Configuring Basic Functions of OSPFv3

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 router ospf 1
DeviceA(config-router)# router-id 1.1.1.1
DeviceA(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 enable
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::1/64
```

```
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 enable
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 address 2001:2::1/64
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 1
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

(2) Perform the following configurations on Device B.

Enable the OSPFv3 process and configure a router ID.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 router ospf 1
DeviceB(config-router)# router-id 2.2.2.2
DeviceB(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 enable
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::2/64
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# ipv6 enable
DeviceB(config-if-GigabitEthernet 0/2)# ipv6 address 2001:3::1/64
DeviceB(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 2
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

(3) Perform the following configurations on Device C.

Enable the OSPFv3 process and configure a router ID.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ipv6 router ospf 1
DeviceC(config-router)# router-id 3.3.3.3
DeviceC(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
DeviceC(config)# interface gigabitethernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# ipv6 enable
DeviceC(config-if-GigabitEthernet 0/3)# ipv6 address 2001:2::2/64
DeviceC(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 1
```

```
DeviceC(config-if-GigabitEthernet 0/3)# exit
```

(4) Perform the following configurations on Device D.

Enable the OSPFv3 process and configure a router ID.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# ipv6 router ospf 1
DeviceD(config-router)# router-id 4.4.4.4
DeviceD(config-router)# exit
```

Configure an IP address for the interface and enable OSPFv3 on the interface.

```
DeviceD(config)# interface gigabitethernet 0/3
DeviceD(config-if-GigabitEthernet 0/3)# ipv6 enable
DeviceD(config-if-GigabitEthernet 0/3)# ipv6 address 2001:3::2/64
DeviceD(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 2
DeviceD(config-if-GigabitEthernet 0/3)# exit
```

5. Verification

(1) Display the following information on Device A.

Display OSPFv3 neighbor information.

```
DeviceA# 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.

```
DeviceA# show ipv6 route ospf

IPv6 routing table name - Default - 0 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, EV - BGP EVPN, N - Nd to host

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.

```
DeviceB# 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.

```
DeviceB# show ipv6 route ospf

IPv6 routing table name - Default - 0 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, EV - BGP EVPN, N - Nd to host

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.

```
DeviceC# 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.

```
DeviceC# show ipv6 route ospf

IPv6 routing table name - Default - 0 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, EV - BGP EVPN, N - Nd to host

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.

```
DeviceD# 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.

```
DeviceD# show ipv6 route ospf

IPv6 routing table name - Default - 0 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, EV - BGP EVPN, N - Nd to host

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.

```
DeviceD# 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.

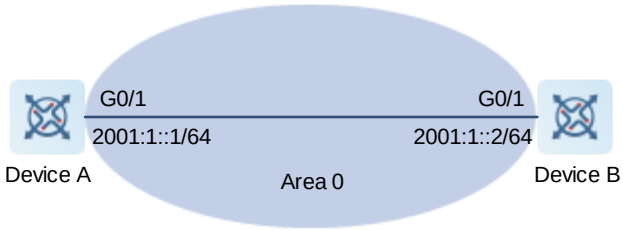
1.22.2 Configuring OSPFv3 Authentication

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf authentication ipsec spi 256 md5
01234567890123456789012345678912
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(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.

```
DeviceA# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State      BFD 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.

```
DeviceB# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State      BFD 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.

1.22.3 Configuring a Stub Area

1. Requirements

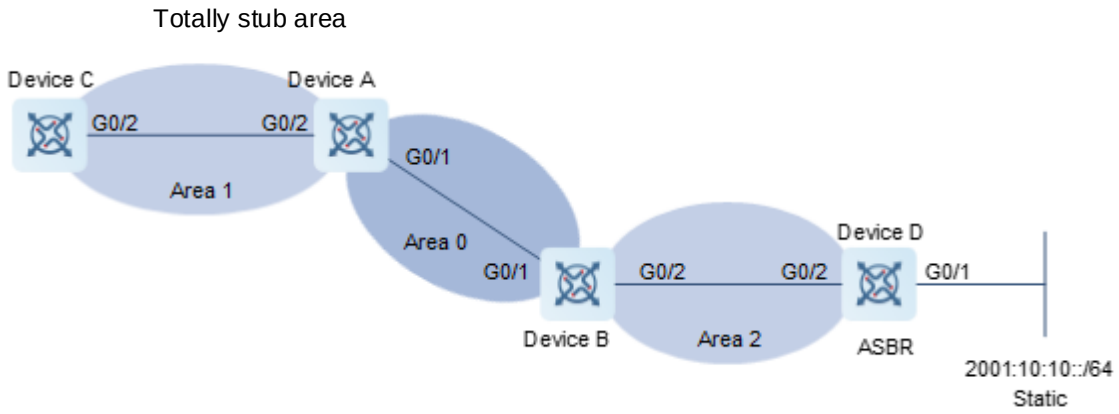
Devices A, B, C, and D are interconnected through the OSPFv3 routing protocol.

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.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# ipv6 router ospf 1
DeviceD(config-router)# redistribute static
```

(3) Configure Area 1 as a stub area on Device A and filter Type 3 LSAs.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 router ospf 1
DeviceA(config-router)# area 1 stub no-summary
```

(4) Configure Area 1 as a stub area on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ipv6 router ospf 1
DeviceC(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.

```
DeviceC# 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.

1.22.4 Configuring an NSSA

1. Requirements

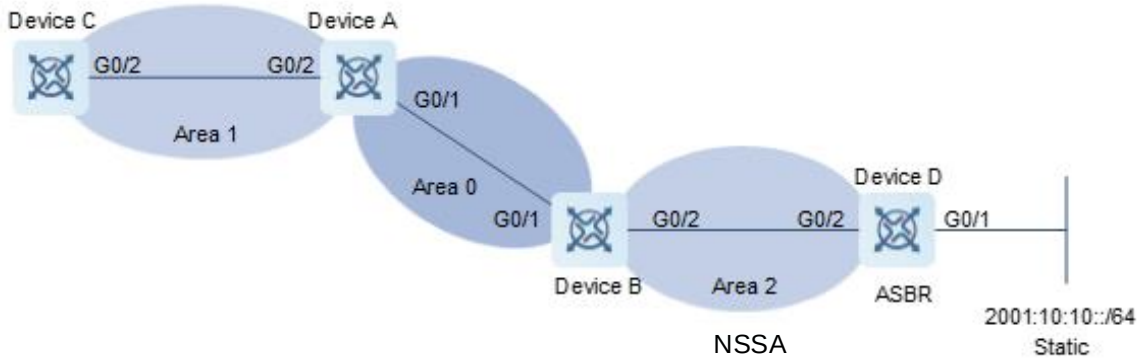
Devices A, B, C, and D are interconnected through the OSPFv3 routing protocol.

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.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# ipv6 router ospf 1
DeviceD(config-router)# area 2 nssa
DeviceD(config-router)# redistribute static
```

(3) Configure Area 2 as an NSSA on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 router ospf 1
DeviceB(config-router)# area 2 nssa
```

5. Verification

(1) Run the **show ipv**6 **ospf database** command on Device D to display the database information and verify that Type 7 LSAs are generated.

```
DeviceD# show ipv6 ospf database nssa-external
          OSPFv3 Router with ID (4.4.4.4) (Process 1)



              NSSA-external-LSA (Area 0.0.0.2)


  LS age: 893
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 4.4.4.4
  LS Seq Number: 0x80000001
  Checksum: 0xF552
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2001:10:10::/64
    Prefix Options: 8 (-|P|-|-|-)
    Forwarding Address: 2001:3::2
```

(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.

```
DeviceA# show ipv6 route ospf


IPv6 routing table name - Default - 0 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, EV - BGP EVPN, N - Nd to host


O  IA  2001:3::/64 [110/2] via FE80::F816:3EFF:FE76:B8D8, GigabitEthernet 0/1
O  E2  2001:10:10::/64 [110/20] via FE80::F816:3EFF:FE76:B8D8, 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.

1.22.5 Selecting an OSPFv3 DR

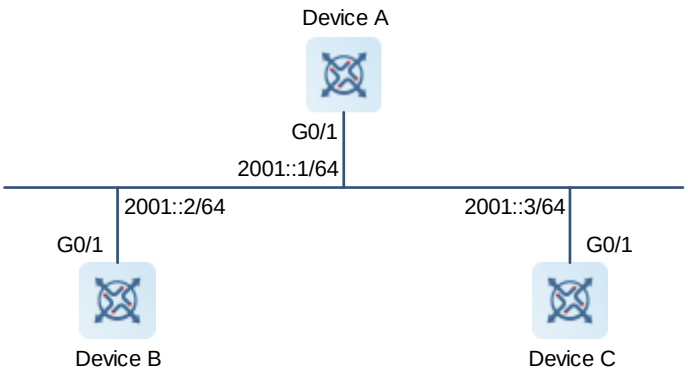
1. Requirements

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.

```
DeviceA> enable
```

```
DeviceA# configure terminal
DeviceA(config)# ipv6 router ospf 1
DeviceA(config-router)# router-id 1.1.1.1
DeviceA(config-router)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 router ospf 1
DeviceB(config-router)# router-id 2.2.2.2
DeviceB(config-router)# exit
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ipv6 router ospf 1
DeviceC(config-router)# router-id 3.3.3.3
DeviceC(config-router)# exit
```

(2) Configure IP addresses of interfaces, configure OSPFv3, and modify the DR election priority of all the devices.

Configure Device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 2001::1/64
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 10
```

Configure Device B.

```
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 address 2001::2/64
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 ospf priority 5
```

Configure Device C.

```
DeviceC(config)# interface gigabitethernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ipv6 address 2001::3/64
DeviceC(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceC(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.

```
DeviceC# 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.

```
DeviceA# 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
!
```

1.22.6 Configuring BFD for OSPFv3

1. Requirements

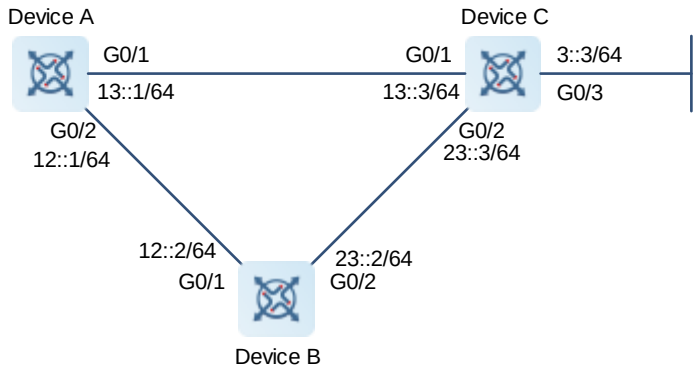
Devices A, B, and C are interconnected through OSPFv3.

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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 address 12::1/64
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 0
DeviceA(config-if-GigabitEthernet 0/2)# exit
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 address 13::1/64
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# ipv6 router ospf 1
DeviceA(config-router)# router-id 1.1.1.1
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 address 12::2/64
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

```
DeviceB(config)# interface gigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# ipv6 address 23::2/64
DeviceB(config)# ipv6 router ospf 1
DeviceB(config-router)# router-id 2.2.2.2
```

Configure Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# interface gigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ipv6 address 13::3/64
DeviceC(config-if-GigabitEthernet 0/1)# ipv6 ospf 1 area 0
DeviceC(config-if-GigabitEthernet 0/1)# exit
DeviceC(config)# interface gigabitEthernet 0/2
DeviceC(config-if-GigabitEthernet 0/2)# ipv6 address 23::3/64
DeviceC(config-if-GigabitEthernet 0/2)# ipv6 ospf 1 area 0
DeviceC(config-if-GigabitEthernet 0/2)# exit
DeviceC(config)# interface gigabitethernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# ipv6 address 3::3/64
DeviceC(config-if-GigabitEthernet 0/3)# ipv6 ospf 1 area 0
DeviceC(config-if-GigabitEthernet 0/3)# exit
DeviceC(config)# ipv6 router ospf 1
DeviceC(config-router)# router-id 3.3.3.3
```

(2) Enable the BFD function in the OSPFv3 routing process mode.

Configure Device A.

```
DeviceA(config-router)# bfd all-interfaces
```

Configure Device B.

```
DeviceB(config-router)# bfd all-interfaces
```

Configure Device C.

```
DeviceC(config-router)# bfd all-interfaces
```

5. Verification

- Normal network environment

Check the routing table of Device A.

```
DeviceA# 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.

```
DeviceA# 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.

```
DeviceA# 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.

```
DeviceA# 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
```

```
!
interface gigabitethernet 0/3
ipv6 address 3::3/64
ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 router-id 3.3.3.3
 graceful-restart
 bfd all-interfaces
!
```

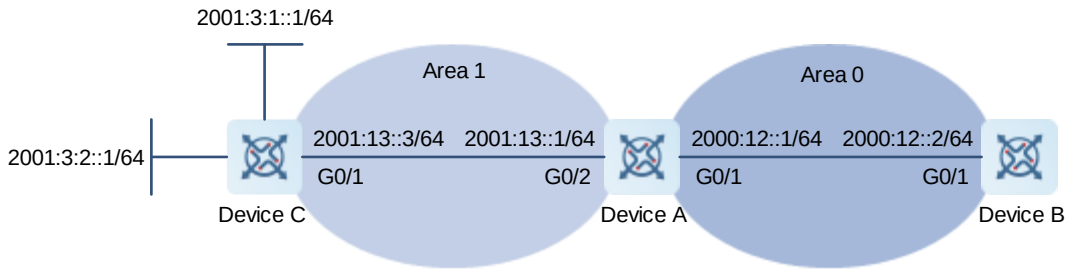
1.22.7 Configuring OSPFv3 Route Summarization

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.

```
DeviceC> enable
DeviceC# configure terminal
```

```
DeviceC(config)# ipv6 router ospf 1
DeviceC(config-router)# redistribute static
DeviceC(config-router)# summary-prefix 2001:3::/32
```

(3) Summarize routes in Area 1 as 2001:13::/32 on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 router ospf 1
DeviceA(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.

```
DeviceA# 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.

```
DeviceB# 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 VRF 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 a Single-protocol VRF 4
1.4.1 Overview 4
1.4.2 Restrictions and Guidelines 4
1.4.3 Configuration Tasks 4
1.4.4 Creating a Single-protocol VRF 4
1.4.5 Configuring the RD for a Single-protocol VRF 5
1.4.6 Configuring the RT for a Single-protocol VRF 5
1.4.7 Configuring an Export Policy Associated with a Single-protocol VRF 6
1.4.8 Configuring an Import Policy Associated with a Single-protocol VRF 6
1.4.9 Adding an Interface to a Single-protocol VRF 7
1.4.10 Importing Routes of an Interface to a Single-protocol VRF 8
1.4.11 Configuring Maximum Number of Routes for a Single-protocol VRF 9
1.5 Configuring a Multi-protocol VRF 9
1.5.1 Overview 9
1.5.2 Restrictions and Guidelines 9
1.5.3 Configuration Tasks 9

1.5.4 Creating a Multi-protocol VRF 10
1.5.5 Configuring the Address Family for a Multi-protocol VRF 10
1.5.6 Configuring the RD for a Multi-protocol VRF 11
1.5.7 Configuring the RT for a Multi-protocol VRF 11
1.5.8 Configuring an Export Policy Associated with a Multi-protocol VRF 12
1.5.9 Configuring an Import Policy Associated with a Multi-protocol VRF 12
1.5.10 Adding an Interface to a Multi-protocol VRF 13
1.5.11 Importing Routes of an Interface to a Multi-protocol VRF 14
1.5.12 Configuring Maximum Number of Routes for a Multi-protocol VRF 15
1.6 VRF Configuring a Global VRF 15
1.6.1 Overview 15
1.6.2 Restrictions and Guidelines 15
1.6.3 Configuration Tasks 15
1.6.4 Configuring the Address Family for a Global VRF 16
1.6.5 Configuring the RD for a Global VRF 16
1.6.6 Configuring the RT for a Global VRF 17
1.6.7 Configuring an Export Policy Associated with a Global VRF 17
1.6.8 Configuring an Import Policy Associated with a Global VRF 18
1.6.9 Configuring Maximum Number of Routes for a Global VRF 18
1.7 Monitoring 19

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 and OSPFv3) 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.*

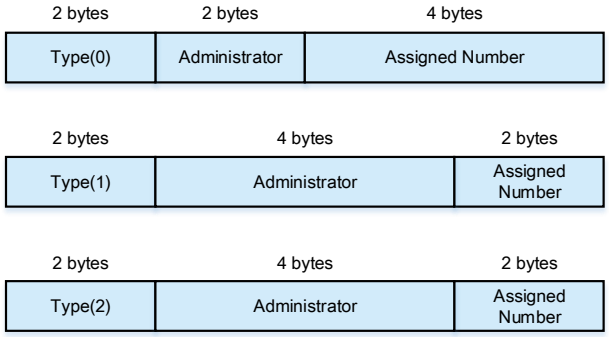
3. VPN Route Attribute

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:

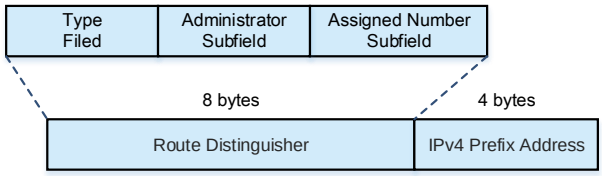
Figure 1-1 RD structure



  - 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



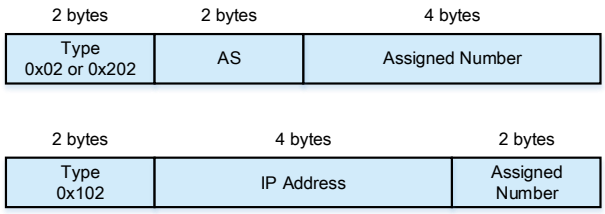
- RT is used to control the advertising and installation policies of VPN routes. The RT attribute falls into the

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.

1.2 Restrictions and Guidelines

- You can configure only one type of VRF: single-protocol VRF or Multi-protocol VRF.
- Single-protocol VRFs only support IPv4, whereas Multi-protocol 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 an Export Policy Associated with a Single-protocol VRF
  - e (Optional)Configuring an Import Policy Associated with a Single-protocol VRF
  - f Adding an Interface to a Single-protocol VRF
  - g (Optional)Importing Routes of an Interface to a Single-protocol VRF
  - h (Optional)Configuring Maximum Number of Routes for a Single-protocol VRF
- Configuring a Multi-protocol VRF
  - a Creating a Single-protocol VRF
  - b (Optional) Configuring the Address Family for a Multi-protocol VRF
  - c (Optional) Configuring the RD for a Single-protocol VRF
  - d (Optional)Configuring the RT for a Single-protocol VRF
  - e (Optional)Configuring an Export Policy Associated with a Multi-protocol VRF
  - f (Optional)Configuring an Import Policy Associated with a Multi-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 Maximum Number of Routes for a Multi-protocol VRF

- VRF Configuring a Global VRF
  a (Optional) Configuring the RD for a Single-protocol VRF
  b (Optional)Configuring the RT for a Single-protocol VRF
  c (Optional)Configuring an Export Policy Associated with a Global VRF
  d (Optional)Configuring an Import Policy Associated with a Global VRF
  e (Optional)Configuring 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 and OSPF) to a VRF.
- Only IPv4 is supported.
- When a Layer 3 interface joins or exits a single-protocol VRF, the IPv4 address, related routing protocols and Layer 3 attributes of the interface will be deleted as well.
- If a Layer 3 interface has been added to a single-protocol VRF, the IPv4 address, related routing protocols, and Layer 3 attributes of the interface will be deleted when the VRF is deleted.

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 an Export Policy Associated with a Single-protocol VRF

(5) (Optional)Configuring an Import Policy Associated with a Single-protocol VRF

(6) Adding an Interface to a Single-protocol VRF

(7) (Optional)Importing Routes of an Interface to a Single-protocol VRF

(8) (Optional)Configuring Maximum Number of Routes for 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 single-protocol VRF configuration mode.

ip vrf *vrf-name*

No single-protocol VRF is configured by default.

(4) (Optional) Configure single-protocol VRF descriptor.

description *description*

By default, no single-protocol VRF descriptor is configured.

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 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.

1.4.8 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.

1.4.9 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

1.4.10 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 import the host route and direct route of an interface to multiple VRFs, run this command multiple times.
- 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.

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 Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *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.

1.4.11 Configuring Maximum Number of Routes for a Single-protocol VRF

2. Overview

You can limit the maximum number of routing entries in a single-protocol VRF by performing this configuration.

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 maximum number of routes in a single-protocol VRF.
maximum routes *limit* { **warning-only** | *warning-threshold* }

The maximum number of routes in a VRF is not configured by default.

1.5 Configuring a Multi-protocol VRF

1.5.1 Overview

This section describes how to configure a Multi-protocol VRF to manage VPN routes. You can configure the address family to support IPv4 and IPv6.

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 Multi-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 and OSPF) to a VRF.
- When a Layer 3 interface joins or exits a multi-protocol VRF, the IPv4 address, related routing protocols and Layer 3 attributes of the interface will be deleted as well.
- If a Layer 3 interface has been added to a multi-protocol VRF, the IPv4 address, related routing protocols, and Layer 3 attributes of the interface will be deleted when the VRF is deleted.

1.5.3 Configuration Tasks

The configuration of a Multi-protocol VRF includes the following tasks:

(1) Creating a Multi-protocol VRF

(2) (Optional) Configuring the Address Family for a Multi-protocol VRF

(3) (Optional) Configuring the RD for a Multi-protocol VRF

(4) (Optional) Configuring the RT for a Multi-protocol VRF

(5) (Optional) Configuring an Export Policy Associated with a Multi-protocol VRF

(6) (Optional) Configuring an Import Policy Associated with a Multi-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 Maximum Number of Routes for a Multi-protocol VRF

1.5.4 Creating a Multi-protocol VRF

1. Overview

This section describes how to create a Multi-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 Multi-protocol VRF, and enter the Multi-protocol VRF configuration mode.

vrf definition *vrf-name*

No Multi-protocol VRF exists by default.

(4) (Optional) Configure multi-protocol VRF descriptor.

description *description*

By default, no multi-protocol VRF descriptor is configured.

1.5.5 Configuring the Address Family for a Multi-protocol VRF

1. Overview

This section describes how to enable the IPv4/IPv6 address family for a Multi-protocol 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 multi-protocol 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 IPv4 address family configuration mode of the multi-protocol VRF.

  address-family ipv4

- Configure the IPv6 address family, and enter the VRF IPv6 address family configuration mode of the multi-protocol VRF.

address-family ipv6

No address family is configured for a Multi-protocol VRF by default.

1.5.6 Configuring the RD for a Multi-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 Multi-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 Multi-protocol 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 Multi-protocol 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 Multi-protocol VRF mode or Multi-protocol 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 Multi-protocol VRF configuration mode.

vrf definition *vrf-name*

- (Optional) Enter the Multi-Protocol VRF address family configuration mode.

address-family { **ipv4** | **ipv6** }

(4) Configure the RT.

route-target { **both** | **export** | **import** } *route-value*

By default, the RT is not configured.

1.5.8 Configuring an Export Policy Associated with a Multi-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 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 Multi-protocol VRF configuration mode.

vrf definition *vrf-name*

(4) Enter the Multi-protocol 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.

1.5.9 Configuring an Import Policy Associated with a Multi-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 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 Multi-protocol VRF configuration mode.

vrf definition *vrf-name*

(4) Enter the Multi-Protocol 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.

1.5.10 Adding an Interface to a Multi-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

- 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 Multi-protocol VRF, enable the address family for the table. If the IPv4 address family is disabled when you add an interface to a Multi-protocol 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 Multi-protocol VRF, you are not allowed to configure the IPv6 and VRRP IPv6 addresses on this interface.
- You must add an interface to the Multi-protocol VRF before configuring the IPv4/IPv6 or VRRP IPv4/IPv6 addresses on the interface. When you add an interface to a Multi-protocol 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 Multi-protocol 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 Multi-protocol 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Add the interface to the Multi-protocol VRF.

vrf forwarding *vrf-name*

By default, an interface does not belong to any VRF.

1.5.11 Importing Routes of an Interface to a Multi-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 import the host route and direct route of an interface to multiple VRFs, run this command multiple times.
- 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.

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 Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Import the host route and direct route of the interface to a specified VRF.

vrf receive *vrf-name*

By default, the host route and direct route of the interface are not imported to a specified VRF.

1.5.12 Configuring Maximum Number of Routes for a Multi-protocol VRF

1. Overview

You can limit the maximum number of routing entries in a multi-protocol VRF by performing this configuration.

2. Procedure

(1) Enter the privileged EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Enter the multi-protocol VRF configuration mode.
vrf definition *vrf-name*

(4) Enter the multi-protocol VRF address family configuration mode.
address-family { **ipv4** | **ipv6** }

(5) Configure the maximum number of routes in a multi-protocol VRF.
maximum routes *limit* { **warning-only** | *warning-threshold* }

The maximum number of routes in a VRF is not configured by default.

1.6 VRF Configuring a Global VRF

1.6.1 Overview

This section describes how to configure a global VRF to manage VPN routes. Global VRF exists 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 and OSPF) to a VRF.

1.6.3 Configuration Tasks

The configuration of a Multi-protocol VRF includes the following tasks:

(1) Configuring the Address Family for a Multi-protocol VRF

(2) (Optional) Configuring the RD for a Multi-protocol VRF

(3) (Optional) Configuring the RT for a Multi-protocol VRF

(4) (Optional)Configuring Maximum Number of Routes 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 l 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 Multi-protocol 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 the global VRF descriptor.

description *description*

By default, no global VRF descriptor is configured.

(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 configuration mode of the global VRF.
  address-family ipv4
- Configure the IPv6 address family, and enter the VRF IPv6 address family configuration mode of the global VRF.
  address-family ipv6

By default, IPv4 and IPv6 address families are enabled.

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 group to control advertisement of VPN routes.

2. Restrictions and Guidelines

- Configure the RT value in global VRF mode or global 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 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*

By default, the RT is not configured.

1.6.7 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 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 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.

1.6.8 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 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 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.

1.6.9 Configuring Maximum Number of Routes for a Global VRF

1. Overview

You can limit the maximum number of routing entries in a global VRF by performing this configuration.

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 in a global VRF.
maximum routes *limit* { **warning-only** | *warning-threshold* }

The maximum number of routes in a VRF is not 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 Multi-protocol VRF.
clear ip mroute [**vrf** *vid*] **statistics** { * | *group-address* [*source-address*] }	Clears the multicast route 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.

Contents

1 Configuring Routing Policies 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Filter List 1
1.1.3 Route Map 2
1.2 Configuration Task Summary 3
1.3 Configuring a Filter List 3
1.3.1 Overview 3
1.3.2 Restrictions and Guidelines 3
1.3.3 Configuration Tasks 3
1.3.4 Creating an IPv4 Prefix List 3
1.3.5 Creating an IPv6 Prefix List 4
1.4 Configuring a Route Map 5
1.4.1 Overview 5
1.4.2 Configuration Tasks 5
1.4.3 Creating a Policy 5
1.4.4 Configuring the Matching Conditions of a Rule 6
1.4.5 Configuring the Processing Actions of a Policy 8
1.4.6 Configuring the Policy Statement 10
1.5 Monitoring 11
1.6 Configuration Examples 12

1.6.1 Applying Rules Configured in a Route Map During Route Redistribution 12

1.6.2 Applying a Route Map in PBR 15

1 Configuring Routing Policies

1.1 Introduction

1.1.1 Overview

In the traditional network, the routing device looks up the routing table according to the destination IP address of the packet, and forwards the packet according to the routing table entry. However, in more and more complex network applications, users expect routing devices to provide more sophisticated and diverse traffic control functions on the basis of traditional route forwarding.

Routing policies are a policy set for changing the packet forwarding path or routing information (routing attributes, next hop, forwarding interface, priority, etc.), 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 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.

1.1.3 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 policies is met, no route is processed according to the route map.
- 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 contains zero match rules, all packets match the policy. If PBR applies a route map, the route map must contain at least one match rule. Otherwise, PBR does not take effect.
  - 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, which are optional. Select tasks for configuration according to actual condition.

(1) Configuring a Filter List

- Creating an IPv4 Prefix List
- Creating an IPv6 Prefix List

(2) Configuring a Route Map

- Creating a Policy
- Configuring the Matching Conditions of a Rule
- Configuring the Processing Actions of a Policy
- (Optional) Configuring the Policy Statement

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, which are optional. Select the configuration tasks as required.

- Creating an IPv4 Prefix List
- Creating an IPv6 Prefix List

1.3.4 Creating an IPv4 Prefix List

1. Overview

An IPv4 prefix list 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 an IPv4 prefix list, and entries are matched based on their sequence numbers. As long as a route matches one entry, the route is permitted by the prefix list and

no further matching is performed. If a route does not match any entry, it is considered that the route is denied by the IPv4 prefix list.

You are advised to add a text description for the IPv4 prefix list, such as the service purpose of the IPv4 prefix list to facilitate maintenance and traceability.

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 an IPv4 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.

(4) (Optional) Add a text description for the IPv4 prefix list.
ip prefix-list *prefix-list-name* **description** *description-text*

By default, no text description is configured for the IPv4 prefix list.

(5) (Optional) Enable the function of displaying sequence numbers in the IPv4 prefix list.
ip prefix-list sequence-number

When you run the **show ip prefix-list** command, the sequence numbers of entries in a prefix list are not displayed by default. When addition or deletion action is performed on an IPv4 prefix list, the sequence numbers of the IPv4 prefix list is displayed for the administrator to intuitively define sequence numbers for the added or deleted items in the IPv4 prefix list.

1.3.5 Creating an IPv6 Prefix List

1. Overview

An IPv6 prefix list 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 an IPv6 prefix list, and entries are matched based on their sequence numbers. As long as a route matches one entry, the route is permitted by the prefix list and no further matching is performed. If a route does not match any entry, it is considered that the route is denied by the IPv6 prefix list.

You are advised to add a text description for the IPv6 prefix list, such as the service purpose of the IPv6 prefix list to facilitate maintenance and traceability.

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.

(4) (Optional) Add a text description for the IPv6 prefix list.
ipv6 prefix-list *prefix-list-name* **description** *descripton-text*

By default, no text description is configured for an IPv6 prefix list.

(5) (Optional) Enable the function of displaying sequence numbers in the IPv6 prefix list.
ipv6 prefix-list sequence-number

When you run the **show ipv6 prefix-list** command, the sequence numbers of entries in a prefix list are not displayed by default. When addition or deletion action is performed on an IPv4 prefix list, the sequence numbers of the IPv4 prefix list is displayed for the administrator to intuitively define sequence numbers for the added or deleted items in the IPv4 prefix list.

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

(4) (Optional) Configuring the Policy Statement

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 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 traffic with the outbound interface.

match interface { *interface-type interface-number* }&<1-4>

By default, a rule is not configured to match traffic with an interface that is used as the next-hop outbound interface.

You can use an IPv4 filter list in the route map to match attributes. The following configurations are optional. You can configure multiple match rules, and all of which must be matched if multiple match rules are configured.

- Configure a rule to match the target network routes that are permitted in the ACL or prefix list.
  match ip address { { *acl-name* | *acl-number* } &<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-name* | *acl-number* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

  By default, no next-hop IPv4 address matching rule is configured.

- Configure a rule to match the target network routes whose source IPv4 addresses meet rules in the ACL or prefix list.

  match ip route-source { { *acl-name* | *acl-number* } &<1-6> | **prefix-list** *prefix-list-name*&<1-6> }

  By default, no rule is configured to match the source IP addresses of routes.

You can use an IPv6 filter list in the route map to match attributes. The following configurations are optional. You can configure multiple match rules, and all of which must be matched if multiple match rules are configured.

- 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.

- Configure a rule to match the target network routes whose next-hop IPv6 addresses meet rules in the ACL or prefix list.

  match ipv6 next-hop { *acl-name* | **prefix-list** *prefix-list-name* }

  By default, no rule to match next-hop IPv6 address of the route is configured.

- 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 rule to match the source IPv6 addresses of routes is configured.

(5) Configure a rule to match the routes with a fixed metric.

match metric *metric*

By default, the metric values of routes are not matched.

(6) Configure a rule to match the route type.

match route-type { **connect** | **external** [**type-1** | **type-2**] | **internal** | **level-1** | **level-2** | **local** | **nssa-external** [**type-1** | **type-2**] | **rip** | **static** } *

By default, no rule is configured to match any route type.

(7) Configure a rule to match the routes with a specified tag.

match tag *tag&*<1-4>

By default, no rule to match the routes with a specified tag is configured.

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 configuring 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 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.

(5) 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 IPv4 address for routes.
  set next-hop *ipv4-address*

  By default, no next-hop IPv4 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>

  By default, no next-hop IPv6 address is specified for a matched route.

- 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.

- 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.

- 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.

- 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.

(8) 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 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.
- Configure the LOCAL_PREFERENCE parameter.
  set local-preference *precedence-number*

  By default, no LOCAL_PREFERENCE value is configured for matched routes.

(9) Configure redistribution-related information.
- Configure the type of the destination area to which redistributed routes are to be advertised.
  set level { backbone | **stub-area** }

  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.

(10) Configure the weight, metric, and metric type.
- Configure the route management distance.
  set distance *distance-number*

  By default, no management distance is modified for matched routes.
- 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** }

(6) Configure the route originator address.

set originator-id *ipv4-address*

By default, no route originator address is configured for matched routes.

1.4.6 Configuring the Policy Statement

1. Overview

Similar to the description of a prefix list, you can configure a statement to describe a route map.

2. Restrictions and Guidelines

- This command is not a routing policy command, and will not be applied to any routing protocol.
- This command takes effect only in OPENCONF YANG, and is used to record the statement name of a route map.
- If this command is not configured, the sequence number of a route map is used as the default statement name of the route map. Therefore, the range from 0 to 65535 is reserved for the **statement-name** command as the default configuration range. Within this range, all the sequence numbers except the sequence number of a route map configured with **statement-name** cannot be used because they are reserved for the sub-route maps with the same name as the route map and used as the default statement content.

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 the statement name for the route map.
statement-name [*name*]

By default, the statement name is the sequence number of the route map.

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.
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*] [**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.

Command	Purpose
show ip as-path-access-list [*as-path-access-list-number*]	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-number* | *extcommunity-list-name*]	Displays the configurations of an extcommunity list.
show rpi	Displays the capability value of a route map.

1.6 Configuration Examples

1.6.1 Applying Rules Configured in a Route Map During Route Redistribution

1. Requirements

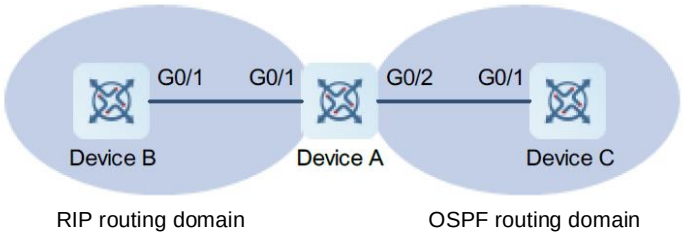
The RIP routing domain needs to exchange routes with the OSPF routing domain to realize the network-wide interworking.

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 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**.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# route-map redrip permit 10
DeviceA(config-route-map)# match metric 4
DeviceA(config-route-map)# set metric-type type-1
DeviceA(config-route-map)# set tag 40
DeviceA(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**.

```
DeviceA(config)# route-map redospf permit 10
DeviceA(config-route-map)# match tag 10
DeviceA(config-route-map)# set metric 10
DeviceA(config-route-map)# exit
```

(4) Configure redistribution of RIP routes to OSPF, and use the route map **redrip** for routing control.

```
DeviceA(config)# router ospf 1
DeviceA(config-router)# redistribute rip subnets route-map redrip
DeviceA(config-router)# exit
```

(5) Configure the redistribution of OSPF routes to RIP, and use the route map **redospf** for routing control.

```
DeviceA(config)# router rip
DeviceA(config-router)# redistribute ospf 1 route-map redospf
DeviceA(config-router)# exit
```

5. Verification

Check the route map configurations on device A to verify the policy rules.

```
DeviceA# show route-map
route-map redrip, permit, sequence 10
  Match clauses:
    metric 4
  Set clauses:
    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.

```
DeviceA# 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

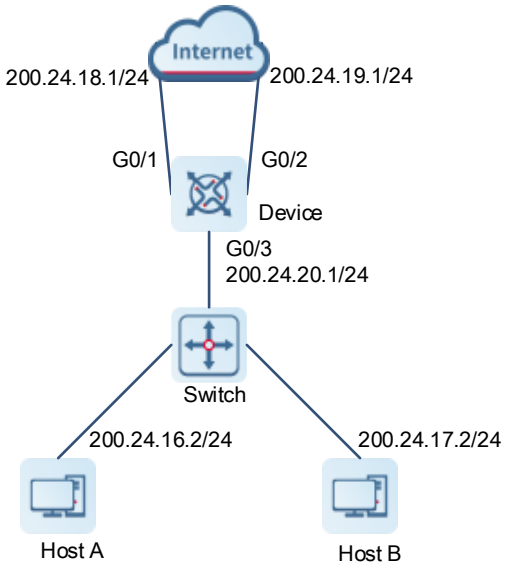
A company's network has dual egresses, which are active and standby egresses. As the network size increases, the active link has insufficient bandwidth at the peak. The IT Department uses the bandwidth resources of the standby link to meet business needs without expanding the bandwidth of the active link.

You can configure the policy-based routing function on the egress device, so that the company traffic is shared by two egresses, and the two egresses act as the standby egress to each other. The diversion rules are as follows:

- 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.

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                    state
GigabitEthernet 0/3                  RM_FOR_PBR                   ok
```

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
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.

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....7
1.3.4 Applying PBR to an Interface....8
1.3.5 Applying PBR to a Local Device....8
1.3.6 Manually Loading PBR Entries....9
1.4 Configuring Redundant Backup or Load Balancing....9
1.4.1 Overview....9
1.4.2 Restrictions and Guidelines....9
1.4.3 Procedure....10
1.5 Configuring Source-Address-Based PBR....11
1.5.1 Overview....11
1.5.2 Restrictions and Guidelines....11
1.5.3 Procedure....11
1.6 Monitoring....12

1.7 Configuration Examples....13

1.7.1 Configuring PBR to Implement Multi-Exit High Availability....13

1.7.2 Selecting an Output Link based on Source Addresses of Packets....17

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

  When PBR applies a route map, the route map must contain at least one matching rule.
  - If the route map contains no matching rule, PBR will not take effect.
  - If the matching condition contains one or more matching 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.

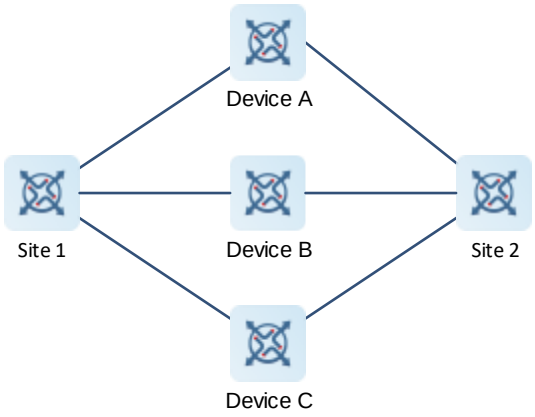
- Redundant backup

  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
   - Manually Loading PBR Entries

(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.
- Match rule use restrictions of PBR in route map:

- IPv4 PBR uses IP standard ACL or extended ACL to define the source IP address (and destination IP address) range in packets.
- IPv6 PBR uses IPv6 extended ACL to define the source IPv6 address (and destination IPv6 address) range in packets.
- If PBR references a nonexistent ACL, the submap of this route is not matched, and the submap of the next route is matched. If no route map is matched, packets are forwarded through a common route. If only ACL is configured but ACE is not, the PBR routing behavior is the same as that in the nonexistent ACL scenario.
- On a switch, the IPv4 PBR interface supports expert extended ACL and MAC extended ACL. Local PBR does not support expert extended ACL or MAC extended ACL.
- On a switch, if one route submap in PBR references multiple ACLs, only the first existent ACL is matched, but the others are not.

Table 1-1 Output Fields of Match Rules Supported by PBR

	Command	Description
IPv4 PBR	**match ip address**	The match condition is the source IPv4 address (and destination IPv4 address). One policy can be configured with only one **match ipv4 address** command.
IPv6 PBR	**match ipv6 address**	The match condition is the source IPv6 address (and destination IPv6 address). One policy can be configured with only one **match ipv6 address** command.

- Set rule use restrictions of PBR in route map:

  Priority: **set ip next-hop** > **set ip next-hop recursive** > common route > **set ip default next-hop** > default route. All the preceding **set** commands can be configured, but only the command with the highest priority takes effect.

  Priority: **set ipv6 next-hop** > **set ipv6 next-hop recursive** > common route > **set ipv6 default next-hop** > default route. All the preceding **set** commands can be configured, but only the command with the highest priority takes effect.

  - On a switch, the **set ipv6 default next-hop** command does not take effect on the IPv6 addresses of which the mask length exceeds 64.

Table 1-2 Output Fields of Set rules Supported by PBR

	Command	Description
IPv4 PBR	**set ip tos**	Modifies the TOS field in IPv4 packets. This command cannot be used together with **set ip dscp** command**.**
	set ip precedence	Modifies the Precedence field in IPv4 packets. This command cannot be used together with **set ip dscp** command**..**

	set ip dscp	Modifies the DSCP field in IPv4 packets. This command cannot be used together with **set ip tos** or **set ip precedence** command**..**
	set ip next-hop	Specifies the next hop address for IPv4 packets. The next hop must be directly connected; otherwise, this command is invalid. The packets matching the Match rules are forwarded to the next hop specified in **set ip next-hop** command**.**, no matter whether the route of the packets specified in the routing table is the same as the next hop specified by PBR. On a switch, the outbound interface of the next hop specified by PBR is an SVI, Layer 3 Ethernet interface, or Layer 3 aggregate interface.
	set ip next-hop recursive	Specifies the next hop of the recursive route for IPv4 packet forwarding. The next hop can be directly or indirectly connected. If the next hop is indirectly connected, the next hop will be recursed to a static or dynamic route in the routing table. This command supports recursing multiple ECMP next hops to static or dynamic routes. A maximum of 32 next hops are supported. If the recursive route is a static route, only one next hop can be recursed to the static route. The redundancy backup mode or load balancing mode of multiple recursive next hops are decided by the **ip policy** { **redundance** | **load-balance** } command. The packet matching the Match rules are forwarded to the next hop specified by **set ip next-hop recursive** command first, no matter whether the route of the packets specified in the routing table is the same as the next hop specified by PBR. The PBR recursive route next hop is valid only when the static or dynamic route has an outbound interface and next hop IP address.
	set ip next-hop verify-availability	Verifies the reachability of the next hop IPv4 address.
	set ip default next-hop	Specifies the default next hop for IPv4 packets. If the routing of the packets matching the Match rules fails or a default route is selected, the packets are forwarded to the default next hop specified in this command.
IPv6 PBR	**set ipv6 precedence**	Modifies the Precedence field in IPv6 packets. IPv6 PBR does not support **set ipv6 tos** or **set ipv6 dscp** command.

	set ipv6 next-hop	Specifies the next hop address for IPv6 packets. The IPv6 packets matching the Match rules are forwarded to the next hop specified in **set ipv6 next-hop** command, no matter whether the route of the IPv6 packets specified in the routing table is the same as the next hop specified by PBR. This command is valid only when the next hop is directly connected.
	set ipv6 next-hop recursive	Specifies the next hop of the recursive route for IPv6 packet forwarding. The next hop can be directly or indirectly connected. If the next hop is indirectly connected, the next hop will be recursed to a static or dynamic route in the routing table. This command supports recursing multiple ECMP next hops to static or dynamic routes. A maximum of 32 next hops are supported. If the recursive route is a static route, only one next hop can be recursed to the static route. The redundancy backup mode or load balancing mode of multiple recursive next hops are decided by the **ipv6 policy** { **redundance** | **load-balance** } command. The packet matching the Match rules are forwarded to the next hop specified by **set ipv6 next-hop recursive** command first, no matter whether the route of the packets specified in the routing table is the same as the next hop specified by PBR. The PBR recursive route next hop is valid only when the static or dynamic route has an outbound interface and next hop IPv6 address.
	set ipv6 next-hop verify-availability	Verifies the reachability of the next hop IPv6 address.
	set ipv6 default next-hop	Specifies the default next hop for IPv6 packets. If the routing of IPv6 packets matching the Match rules fails or a default route is selected, the IPv6 packets are forwarded to the next hop specified in this command. This command is valid only when the next hop is directly connected.

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
- Manually Loading PBR Entries

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the SVI configuration mode.

  interface vlan *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.

1.3.6 Manually Loading PBR Entries

1. Overview

This function is used to restore PBR entries in fault scenarios. For example, PBR entries may fail to be loaded on hardware due to routing table overflow and PBR entries may be discarded due to insufficient memory and other reasons. After the number of routes decreases or the memory usage returns to normal, you can use this function to restore the PBR entries on hardware.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Synchronize software IPv4 PBR entries to hardware.

ip policy-sync all

(4) Synchronize software IPv6 PBR entries to hardware.

ipv6 policy-sync all

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 1-3 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**.
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** *ipv4-address*

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure applying source address policy routing for IPv4 packets received by the interface.

ip policy-source in-interface *interface-type interface-number sequence* { *source-address mask* | *source-address/mask* } [**default**] **next-hop** { *ipv4-address* [*weight*] } &<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>

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 1-4 Monitoring of the PBR

Command	Purpose
show access-list	Displays the configurations of an ACL.
show ip pbr bfd	Displays the correlation between the IPv4 PBR and BFD.
show ip pbr recursive	Displays routing information after IPv4 PBR next-hop recursion.
show ip pbr route [**interface** *interface-type interface-number* | **local**]	Displays the routing information of the IPv4 PBR.
show ip pbr route-map *rmap-name*	Displays a route map used by the IPv4 PBR.
show ip pbr source-route [**interface** *interface-type interface-number*]	Displays the routing information of source-address-based IPv4 PBR.
show ip pbr statistics [**interface** *interface-type interface-number* | **local**]	Displays the statistics about the IPv4 PBR.
show ip pbr track	Displays the correlation between PBR and Track.
show ip policy [*route-map-name*]	Displays the configurations of the IPv4 PBR.
show ipv6 pbr bfd	Displays the correlation between the IPv6 PBR and BFD.
show ipv6 pbr recursive	Displays routing information after IPv6 PBR next-hop recursion.

show ipv6 pbr route [**interface** *interface-type interface-number* | **local**]	Displays the routing information of the IPv6 PBR.
show ipv6 pbr route-map *rmap-name*	Displays a route map used by the IPv6 PBR.
show ipv6 pbr source-route [**interface** *interface-type interface-number*]	Displays the routing information of source-address-based IPv6 PBR.
show ipv6 pbr statistics [**interface** *interface-type interface-number* | **local**]	Displays the statistics about the IPv6 PBR.
show ipv6 policy	Displays the configurations of the IPv6 PBR.
show route-map [*name*]	Displays the configurations of a route map.
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.
debug pbr ms	Debugs multiple service cards supported by PBR.
debug pbr msg	Debugs PBR message communication.
debug pbr nsm	Debugs the correlation 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

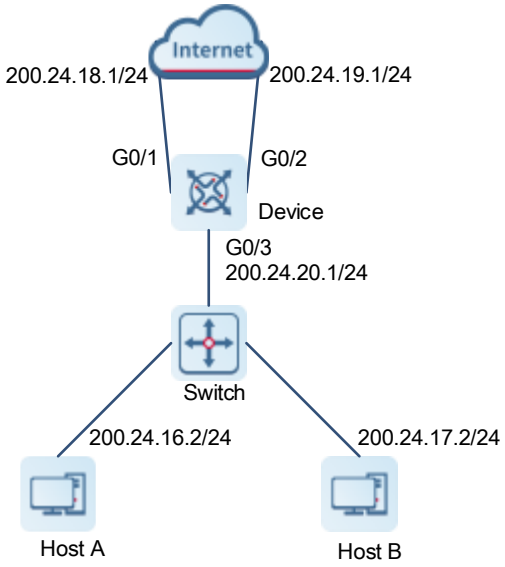
Configure PBR on the devices to achieve the following purposes:

- 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 Topology of PBR Implementing Multi-Exit High Availability



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                    state
GigabitEthernet 0/3                  RM_FOR_PBR                   ok
```

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 verify-availability 200.24.18.1 track 1
```

```
   ip next-hop verify-availability 200.24.19.1 track 2
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ip address 2
  Set clauses:
    ip next-hop verify-availability 200.24.19.1 track 2
    ip next-hop verify-availability 200.24.18.1 track 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
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

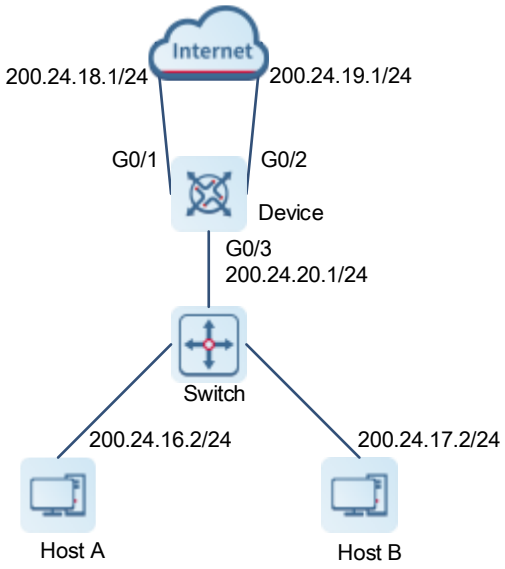
1. Requirements

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 Routing 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 a Key Authentication Algorithm 4

1.2.8 Configuring the Send-Lifetime 5

1.2.9 Configuring the Accept-Lifetime 5

1.2.10 Configuring the Maximum Number of Keys 6

1.3 Monitoring 6

1.4 Configuration Examples 7

1.4.1 Configuring Key Authentication 7

1 Configuring Routing 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

- Keys are used only for RIP and OSPF 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 a Key Authentication Algorithm

(5) (Optional) Configuring the Send-Lifetime

(6) (Optional) Configuring the Accept-Lifetime

(7) (Optional) Configuring the Maximum Number of Keys

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 a Key Authentication Algorithm

1. Overview

The TCP enhanced authentication option type do not have a unified standard. This affects communication between devices of different vendors when these devices are used together. Therefore, you need to manually specify the mapping between the authentication algorithm and algorithm ID, and the TCP enhanced authentication option type, both of which are used by the peer device.

2. Restrictions and Guidelines

The **tcp-algorithm-id** and **tcp-algorithm-id** commands apply to authentication of TCP connections.

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) (Optional) Configure the authentication parameters for the TCP connection.

- Specify the mapping between the authentication algorithm and algorithm ID in the TCP enhanced authentication configuration.

  tcp-algorithm-id *algortithm-type algorithm-id*

  By default, the default algorithm ID is used. For example, the default algorithm ID of the SM3 algorithm is **9**.

- Specify the authentication option type in the TCP enhanced authentication configuration.

  tcp-kind *kind-value*

  By default, the authentication option type is **254**.

(5) Specify an authentication algorithm for the specified key.

authentication-algorithm *algortithm-type*

By default, no authentication algorithm is defined.

1.2.8 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.

accept-lifetime *start-time* { *end-time* | **duration** *duration-time* | **infinite** }

By default, the accept-lifetime of a key chain is disabled.

1.2.9 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.

send-lifetime *start-time* { *end-time* | **duration** *duration-time* | **infinite** }

By default, the send-lifetime of a key chain is disabled.

1.2.10 Configuring the Maximum Number of Keys

1. Overview

This section describes how to configure the maximum number of keys to control the key quantity in a key chain.

2. Restrictions and Guidelines

The maximum number of keys cannot be smaller than the current number of configured keys. Before configuring the maximum number of keys, you must delete keys to ensure that the number of configured keys is smaller than the maximum number of keys to be configured.

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) Configure the maximum number of keys.

key-limit *limit-number*

By default, the maximum number of keys in a key chain is **1024**.

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 Key Authentication

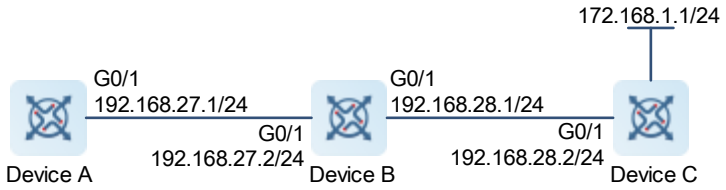
1. Requirements

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 Key Authentication Topology



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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.27.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.27.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure keys and lifetime of each key.

Configure Device A.

```
DeviceA# configure terminal
DeviceA(config)# key chain ripchain
DeviceA(config-keychain)# key 1
DeviceA(config-keychain-key)# key-string Hello
DeviceA(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2013 duration 43200
DeviceA(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2013 duration 43200
DeviceA(config-keychain-key)# exit
DeviceA(config-keychain)# key 2
DeviceA(config-keychain-key)# key-string World
DeviceA(config-keychain-key)# accept-lifetime 04:00:00 Oct 2 2013 infinite
DeviceA(config-keychain-key)# send-lifetime 04:00:00 Oct 2 2013 infinite
DeviceA(config-keychain-key)# exit
```

Configure Device B.

```
DeviceB# configure terminal
DeviceB(config)# key chain ripchain
DeviceB(config-keychain)# key 1
DeviceB(config-keychain-key)# key-string Hello
DeviceB(config-keychain-key)# accept-lifetime 16:30:00 Oct 1 2013 duration 43200
DeviceB(config-keychain-key)# send-lifetime 16:30:00 Oct 1 2013 duration 43200
DeviceB(config-keychain-key)# exit
DeviceB(config-keychain)# key 2
DeviceB(config-keychain-key)# key-string World
DeviceB(config-keychain-key)# accept-lifetime 04:00:00 Oct 2 2013 infinite
DeviceB(config-keychain-key)# send-lifetime 04:00:00 Oct 2 2013 infinite
DeviceB(config-keychain-key)# exit
```

(3) Configure the basic RIP.

Configure Device A.

```
DeviceA(config)# router rip
DeviceA(config-router)# version 2
DeviceA(config-router)# network 192.168.27.0
DeviceA(config-router)# exit
```

Configure Device B.

```
DeviceB(config)# router rip
```

```
DeviceB(config-router)# version 2
DeviceB(config-router)# network 192.168.27.0
DeviceB(config-router)# redistribute static
DeviceB(config-router)# exit
```

(4) Set the interface authentication mode to MD5, and specify the authentication key chain.

Configure Device A.

```
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain ripchain
DeviceA(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
```

Configure Device B.

```
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain ripchain
DeviceB(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5
```

5. Verification

Check whether Device A can receive routes from Device B.

```
DeviceA# 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 7 $10$048$AbuGnns=$
  accept-lifetime 16:30:00 Oct 1 2013 duration 43200
  send-lifetime 16:30:00 Oct 1 2013 duration 43200
 key 2
  key-string 7 $10$3bf$AJJFvvw=$
  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 7 $10$048$AbuGnns=$
  accept-lifetime 16:30:00 Oct 1 2013 duration 43200
  send-lifetime 16:30:00 Oct 1 2013 duration 43200
key 2
  key-string 7 $10$3bf$AJJFvvw=$
  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.

VPN Configuration

1. Configuring IPsec

Contents

1 Configuring IPsec 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Basic Concepts 1

1.1.3 IPsec Tunnel 4

1.1.4 Protocols and Standards 4

1.2 Restrictions and Guidelines 5

1.3 Configuring an IPsec Tunnel for Routing Protocol Authentication 5

1.3.1 Overview 5

1.3.2 Restrictions and Guidelines 5

1.3.3 Configuration Task Summary 5

1.3.4 Configuring an IPsec Proposal 5

1.3.5 Configuring an IPsec SA 6

1.3.6 Applying the IPsec SA to a Routing Protocol 6

1.4 Monitoring 7

1.5 Configuration Examples 7

1.5.1 Configuring an IPsec Tunnel for Routing Protocol Authentication 7

1 Configuring IPsec

1.1 Introduction

1.1.1 Overview

Internet Protocol version 4 (IPv4) is the most widely used network protocol. However, security is not taken into consideration in the design of this protocol. Malicious users can forge addresses of IP packets, tamper with packet content, retransmit the same IP packets repeatedly, and intercept and check packet content at will, which brings many security risks to networks.

IP Security (IPsec) is an L3 tunnel encryption protocol formulated by the Internet Engineering Task Force (IETF). It provides high-quality, interoperable, and cryptography-based security guarantee for data transmitted over networks. Communication parties use IPsec to encrypt and authenticate data sources at the IP layer, in a bid to ensure communication security. IPsec provides the following security services:

- Data confidentiality: An IPsec sender encrypts packets before sending them over a network.
- Data integrity: An IPsec receiver authenticates packets sent by a sender to ensure that data is not tampered with during transmission.
- Data source authentication: An IPsec receiver authenticates an IPsec sender.
- Anti-replay: An IPsec receiver can detect and reject outdated or duplicate packets.

1.1.2 Basic Concepts

1. Security Association

IPsec provides secure communication between two endpoints, which are called IPsec peers.

Security associations (SAs) are the foundation and essence of IPsec. An SA is an agreement on certain elements between communication peers, such as the protocol to be used (Authentication Header (AH), Encapsulating Security Payload (ESP), or both), protocol encapsulation mode (transport mode or tunnel mode), encryption algorithm (Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES)), authentication algorithm (secure hash algorithm (SHA) or message digest algorithm 5 (MD5)), shared keys used to protect data in a specific flow, and key lifetime.

An SA is unidirectional but communication between two peers is bidirectional. At least one SA is needed to protect the data flow in each direction. Therefore, at least two SAs are required for secure communication between two peers. If two peers use both AH and ESP for secure communication, each peer constructs an independent SA for each protocol.

An SA is uniquely identified by a triplet, which contains the security parameter index (SPI), destination IP address, and security protocol number (AH or ESP). An SPI is a 32-bit value that uniquely identifies an SA and is transmitted in the AH and ESP headers.

SAs can be generated via manual configuration and automatic IKE negotiation.

- Manual configuration: You need to run commands to configure all information about an SA. This mode is independent of IKE but you need to update keys periodically to ensure security. The manual mode is applicable to small-sized static networking environments.

- IKE automatic negotiation: An SA is automatically generated and maintained by IKE. The configuration is simpler and this mode is more scalable than the manual mode. IKE automatic negotiation is applicable to large-sized dynamic networking environments.

Manually configured SAs never age whereas SAs automatically negotiated by IKE are valid in their lifetime. There are two types of lifetime:

- Time-based lifetime: Defines the duration from the establishment to expiration of an SA.
- Traffic-based lifetime: Defines the maximum traffic that can be processed by an SA.

You can configure both time-based and traffic-based SA lifetime. An SA will expire once its lifetime reaches the specified time or traffic. Before an SA expires, IKE negotiates and establishes a new SA for IPsec to ensure that the new SA is ready before the expiration of the old SA. The old SA is still used to protect communication before the new SA is successfully negotiated. The new SA is used to protect communication immediately after it is successfully negotiated.

2. Security Protocols

IPsec implements security services by using the following two protocols:

- AH: The protocol number is 51. This protocol provides data source authentication, data integrity verification, and packet replay prevention. Available authentication algorithms include MD5 and Secure Hash Algorithm 1 (SHA-1). AH ensures the integrity and authenticity of data packets, and prevents hackers from intercepting data packets or inserting forged data packets into the network.
- ESP: The protocol number is 50. Different from AH, ESP encrypts user data to be protected and then encapsulates the data into IP packets to ensure data confidentiality. Common encryption algorithms include DES, 3DES, and AES. In addition, you can use the MD5 or SHA-1 algorithm to ensure packet integrity and authenticity.

Table 1-1 Comparison Between AH and ESP

Security Service	AH	ESP
Data confidentiality	Not supported	Supported
Data integrity	Supported (entire IP packet)	Supported (excluding the IP header)
Data source authentication	Supported	Supported
Anti-replay	Supported	Supported

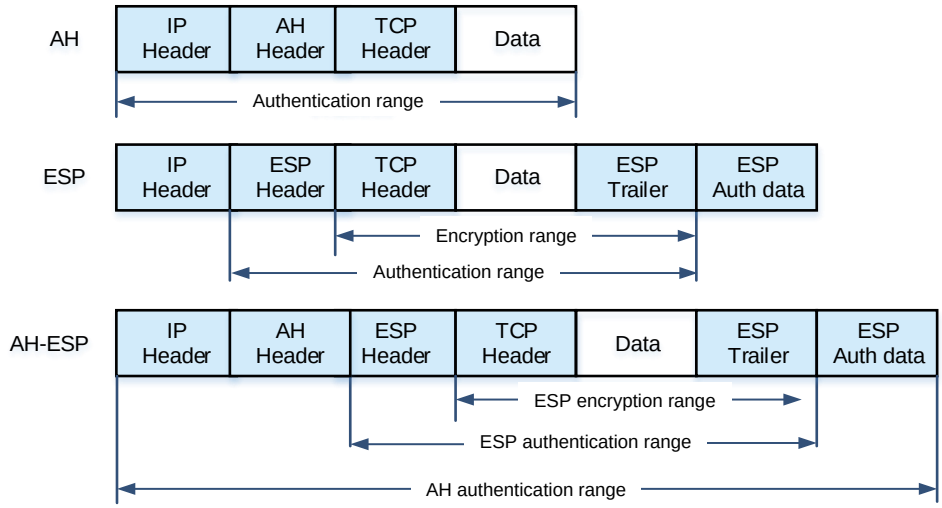
AH and ESP can be used independently or in combination. The device supports the combination of AH and ESP as follows: The device encapsulates packets through ESP and then uses AH to encapsulate packets. If you use AH first and then ESP, the length of a data packet will be changed due to the header, trailer, and padding fields of ESP. However, AH authenticates the entire IP data packet, and an authentication failure is caused.

3. Encapsulation Mode

IPsec supports two work modes:

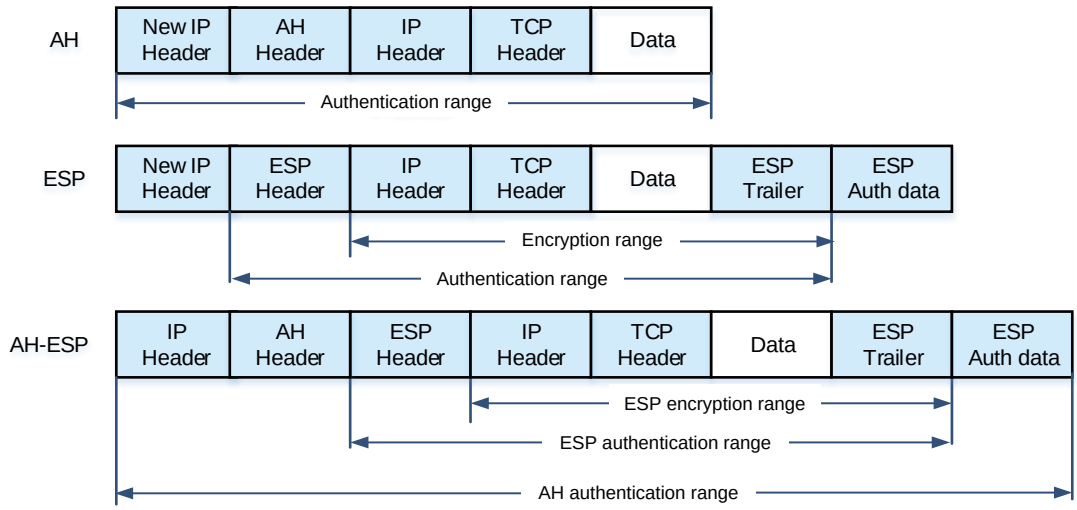
- Transport mode: The AH or ESP header and ESP-encrypted user data are placed after the original IP packet header. The transport mode is typically applied in the communication between two hosts.

Figure 1-1 Packet Encapsulation in Transport Mode



- Tunnel mode: The AH or ESP header and ESP-encrypted user data are encapsulated into a new IP packet. The tunnel mode is typically applied in the communication between two security gateways.

Figure 1-2 Packet Encapsulation in Tunnel Mode



4. Authentication Algorithm

The authentication algorithm is mainly implemented using a hash function. The hash function can accept the input of messages of any length and output a message digest of a fixed length. IPsec peers compute digests separately. If the two digests are the same, a packet is intact and not tampered with. IPsec uses the following authentication algorithms:

- MD5: Generates a 128-bit message digest based on an input message of any length.
- SHA-1: Generates a 160-bit message digest based on an input message with the bit length less than the 64th power of 2.

- SHA2-256: Generates a 256-bit message digest based on an input message with the bit length less than the 64th power of 2.
- SHA2-384: Generates a 384-bit message digest based on an input message with the bit length less than the 128th power of 2.
- SHA2-512: Generates a 512-bit message digest based on an input message with the bit length less than the 128th power of 2.
- SM3: Generates a 256-bit message digest based on an input message with the bit length less than the 64th power of 2.

A longer message digest indicates higher security and slower computation.

5. Encryption Algorithm

IPsec adopts encryption algorithms using symmetric keys, and encrypts and decrypts data with the same key. Currently, IPsec on the device supports three encryption algorithms:

- DES: Encrypts 64-bit plaintext by using a 56-bit key.
- 3DES: Encrypts plaintext by using three 56-bit DES keys.
- AES: Encrypts plaintext by using a 128-bit, 192-bit, or 256-bit key.

1.1.3 IPsec Tunnel

You can configure a static tunnel policy on the CLI to create a common manual tunnel. In the establishment of a tunnel via IKE negotiation, an IKE-encrypted tunnel is established through IKE and then an IPsec tunnel is negotiated through the IKE tunnel. The IKE tunnel and IPsec tunnel are independent of each other. If the IKE tunnel is deleted, the IPsec tunnel still exists. Likewise, the IKE tunnel can exist independently after the IPsec tunnel is deleted. Therefore, IPsec tunnel-related control takes effect only on IPsec tunnels.

1.1.4 Protocols and Standards

- RFC 2401: Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998. (Format: TXT=168162 bytes) (Obsoletes RFC 1825) (Obsoleted by RFC 4301) (Updated by RFC 3168) (Status: PROPOSED STANDARD)
- RFC 2402: IP Authentication Header. S. Kent, R. Atkinson. November 1998. (Format: TXT=52831 bytes) (Obsoletes RFC 1826) (Obsoleted by RFC 4302, RFC 4305) (Status: PROPOSED STANDARD)
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13578 bytes) (Status: PROPOSED STANDARD)
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13089 bytes) (Status: PROPOSED STANDARD)
- RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy. November 1998. (Format: TXT=20208 bytes) (Status: PROPOSED STANDARD)
- RFC 2406: IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998. (Format: TXT=54202 bytes) (Obsoletes RFC 1827) (Obsoleted by RFC 4303, RFC 4305) (Status: PROPOSED STANDARD)
- RFC 3948: UDP Encapsulation of IPsec ESP Packets. A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg. January 2005. (Format: TXT=30366bytes) (Status: PROPOSED STANDARD)

1.2 Restrictions and Guidelines

- Interesting flows in transport mode must be in host-host mode. Otherwise, negotiation is carried out as the flows are in tunnel mode.
- Interesting flow conflicts cannot be detected. Interesting flows specified in static crypto map entries are matched based on the configuration sequence. Dynamic crypto map entries learned or configured later have a higher priority for matching.

1.3 Configuring an IPsec Tunnel for Routing Protocol Authentication

1.3.1 Overview

IPsec authentication is used to authenticate sending and receiving of routing protocol packets to prevent attacks on the device from forged routing protocol packets.

1.3.2 Restrictions and Guidelines

- One IPsec proposal can be applied to multiple IPsec SAs.
- One IPsec SA can be applied to multiple routing protocols.

1.3.3 Configuration Task Summary

IPsec tunnel configuration for routing protocol authentication includes the following tasks:

(1) Configuring an IPsec proposal

(2) Configuring an IPsec SA

(3) Applying the IPsec SA to a routing protocol

1.3.4 Configuring an IPsec Proposal

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Define an IPsec proposal for IPsec SA and enter the IPsec proposal configuration mode.

ipsec proposal proposal-name

The IPsec proposal for IPsec SA is not defined by default.

(4) Configure an encapsulation mode.

encapsulation-mode { transport | tunnel }

No encapsulation mode is configured by default.

(5) Configure a security protocol.

transform { ah | ah-esp | esp }

No security protocol is configured by default.

(6) (Optional) Configure an authentication algorithm for the AH protocol.

ah authentication-algorithm { **md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3** }

No authentication algorithm is configured for the AH protocol by default.

(7) (Optional) Configure an authentication algorithm for the ESP protocol.

esp authentication-algorithm { **md5 | sha1 | sha2-256 | sha2-384 | sha2-512 | sm3** }

No authentication algorithm is configured for the ESP protocol by default.

(8) (Optional) Configure an encryption algorithm for the ESP protocol.

esp encryption-algorithm { **3des | aes-128 | aes-192 | aes-256 | des** }

No encryption algorithm is configured for the ESP protocol by default.

1.3.5 Configuring an IPsec SA

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an IPsec SA and enter the IPsec SA configuration mode.

ipsec sa *sa-name*

No IPsec SA is created by default.

(4) Configure an IPsec proposal for the IPsec SA.

proposal *proposal-name*

No IPsec proposal is configured for the IPsec SA by default.

(5) Configure a security parameter index (SPI) for the IPsec SA.

sa spi { **ah** *spi* | **esp** *spi* }

No SPI is configured by default.

(6) (Optional) Configure an authentication key in hexadecimal notation.

sa authentication-hex { **ah** [**0** | **7**] *hex-key* | **esp** [**0** | **7**] *hex-key* }

No authentication key in hexadecimal notation is configured by default.

(7) (Optional) Configure an authentication key string.

sa string-key { **ah** [**0** | **7**] *string-key* | **esp** [**0** | **7**] *string-key* }

No authentication key string is configured by default.

(8) (Optional) Configure an encryption key in hexadecimal notation.

sa encryption-hex esp [**0** | **7**] *encryption-key*

No encryption key in hexadecimal notation is configured by default.

1.3.6 Applying the IPsec SA to a Routing Protocol

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

- Enter the loopback interface configuration mode.

  interface loopback *interface-number*

(4) Associate SA authentication with an interface.

ipv6 ospf ipsec sa { **disable** | *sa-name* } [**instance** *instance-id*]

No interface is associated with SA authentication 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 **clear** command to clear information.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.
- Running the **clear** command may lose vital information and thus interrupt services.

Table 1-2 IPsec Monitoring

Command	Purpose
show ipsec manual sa [*sa-name*]	Displays information about a configured IPsec SA.
show ipsec proposal [*proposal-name*]	Displays information about a configured IPsec proposal.

1.5 Configuration Examples

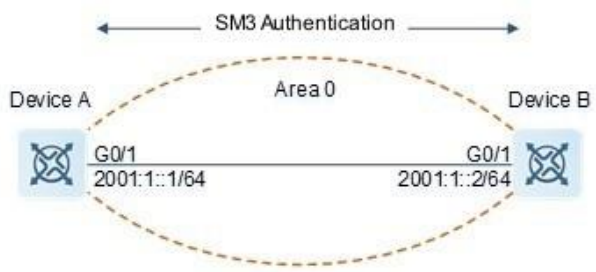
1.5.1 Configuring an IPsec Tunnel for Routing Protocol Authentication

1. Requirements

The customer wants to use SM3 authentication for OSPFv3.

2. Topology

Figure 1-3 Configuring an IPsec Tunnel for Routing Protocol Authentication



3. Notes

- Enable IPv6 on all device interfaces.
- Configure basic OSPFv3 features on all devices.
- Configure OSPFv3 IPsec authentication on all device interfaces.

4. Procedure

(4) Configure Device A.

Start an OSPFv3 process and configure a router ID.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 router ospf 1
DeviceA(config-router)# router-id 1.1.1.1
DeviceA(config-router)# exit
```

Configure an IPsec proposal.

```
DeviceA(config)# ipsec proposal proposal111
DeviceA(config-ipsec-proposal)# encapsulation-mode transport
DeviceA(config-ipsec-proposal)# transform ah
DeviceA(config-ipsec-proposal)# ah authentication-algorithm sm3
DeviceA(config-ipsec-proposal)# exit
```

Configure an IPsec SA.

```
DeviceA(config)# ipsec sa sa1
DeviceA(config-ipsec-sa)# proposal proposal111
DeviceA(config-ipsec-sa)# sa spi ah 256
DeviceA(config-ipsec-sa)# sa authentication-hex ah
0123456789012345678901234567890123456789012345678901234567890123456789abcd
DeviceA(config-ipsec-sa1)# exit
```

Configure an IP address for an interface and configure OSPFv3 on the interface.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1) ipv6 enable
```

```
DeviceA(config-if-GigabitEthernet 0/1) ipv6 address 2001:1::1/64
DeviceA(config-if-GigabitEthernet 0/1) ipv6 ospf 1 area 0
```

Apply the IPsec SA to the routing protocol.

```
DeviceA(config-if-GigabitEthernet 0/1)# ipv6 ospf ipsec sa sa1
```

(5) Configure Device B.

Start an OSPFv3 process and configure a router ID.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipv6 router ospf 1
DeviceB(config-router)# router-id 2.2.2.2
DeviceB(config-router)# exit
```

Configure an IPsec proposal.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ipsec proposal proposal111
DeviceB(config-ipsec-proposal)# encapsulation-mode transport
DeviceB(config-ipsec-proposal)# transform ah
DeviceB(config-ipsec-proposal)# ah authentication-algorithm sm3
DeviceB(config-ipsec-proposal)# exit
```

Configure an IPsec SA.

```
DeviceB(config)# ipsec sa sa1
DeviceB(config-ipsec-sa)# proposal proposal111
DeviceB(config-ipsec-sa)# sa spi ah 256
DeviceB(config-ipsec-sa)# sa authentication-hex ah
0123456789012345678901234567890123456789012345678901234567890123456789abcd
DeviceB(config-ipsec-sa)# exit
```

Configure an IP address for an interface and configure OSPFv3 on the interface.

```
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1) ipv6 enable
DeviceB(config-if-GigabitEthernet 0/1) ipv6 address 2001:1::2/64
DeviceB(config-if-GigabitEthernet 0/1) ipv6 ospf 1 area 0
```

Apply the IPsec SA to the routing protocol.

```
DeviceB(config-if-GigabitEthernet 0/1)# ipv6 ospf ipsec sa sa1
```

5. Verification

Check information about the configured IPsec SA.

```
DeviceA# show ipsec manual sa sa1
ip security association name sa1(len 3), ref 0
  id: 2048(Activated)
  proposal name: proposal111
    encapsulation mode: transport
    transform: ah
    AH protocol: authentication sm3
```

```
   ESP protocol: authentication none, encryption none
  AH setting:
   AH spi: 256 (0x100)
   AH string-key:
   AH authentication hex key:
$10$181$huzuRca9EbwlWTHlMox5plYAfxdN7KC/5vaqeafY8QOjiAr0XjqBD3l6qBal1f6VzI95hKUGD
/VdZFd96drCwQ==$
  ESP setting:
   ESP spi: 0 (0x0)
   ESP string-key:
   ESP encryption hex key:
   ESP authentication hex key:
```

Check whether the OSPF neighbor status is correct on Device A.

```
DeviceA# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State       BFD State     Dead Time   Instance ID   Interface
2.2.2.2          1   Full/DR     -           00:00:38    0           GigabitEthernet
0/1
```

Check whether the OSPF neighbor status is correct on Device B.

```
DeviceB# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID     Pri   State       BFD 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

```
hostname DeviceA
!
ipsec proposal proposal111
 encapsulation-mode transport
 transform ah
 ah authentication-algorithm sm3
!
ipsec sa sa1
 proposal proposal111
 sa spi ah 256
 sa authentication-hex ah 7
$10$019$O9nTeIgui7CbICSsRvbHgROzFLJaegdEAXPBjmiyLPVekQiznSmx69QTO9+VrB/xRMptvc
9KqkZkRtqfdD/OkQ==$
!
interface GigabitEthernet 0/1
 ipv6 enable
 ipv6 address 2001:1::1/64
 ipv6 ospf 1 area 0
```

```
 ipv6 ospf ipsec sa sa1
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ipsec proposal proposal111
 encapsulation-mode transport
 transform ah
 ah authentication-algorithm sm3
!
ipsec sa sa1
 proposal proposal111
 sa spi ah 256
 sa authentication-hex ah 7
$10$019$O9nTeIgui7CbICSsRvbHgROzFLJaegdEAXPBjmiyLPVekQiznSmx69QTO9+VrB/xRMptvc
9KqkZkRtqfdD/OkQ==$
!
interface GigabitEthernet 0/1
 ipv6 enable
 ipv6 address 2001:1::2/64
 ipv6 ospf 1 area 0
 ipv6 ospf ipsec sa sa1
!
ipv6 router ospf 1
 router-id 2.2.2.2
!
end
```

ACL and QoS Configuration

1. Configuring ACL
2. Configuring QoS

Contents

1 Configuring ACL 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Restrictions and Guidelines 13

1.3 Configuration Task Summary 13

1.4 Configuring an IP Standard ACL 13

1.4.1 Overview 13

1.4.2 Restrictions and Guidelines 14

1.4.3 Configuration Tasks 14

1.4.4 Creating an IP Standard ACL 14

1.4.5 Applying an IP Standard ACL 16

1.5 Configuring an IP Extended ACL 17

1.5.1 Overview 17

1.5.2 Restrictions and Guidelines 17

1.5.3 Configuration Tasks 17

1.5.4 Creating an IP Extended ACL 17

1.5.5 Applying an IP Extended ACL 19

1.6 Configuring a MAC Extended ACL 21

1.6.1 Overview 21

1.6.2 Restrictions and Guidelines 21

1.6.3 Configuration Tasks 21

1.6.4 Creating a MAC Extended ACL 21

1.6.5 Applying a MAC Extended ACL 23
1.7 Configuring an Expert Extended ACL 24
1.7.1 Overview 24
1.7.2 Restrictions and Guidelines 24
1.7.3 Configuration Tasks 24
1.7.4 Creating an Expert Extended ACL 24
1.7.5 Applying an Expert Extended ACL 26
1.8 Configuring an IPv6 ACL 27
1.8.1 Overview 27
1.8.2 Restrictions and Guidelines 27
1.8.3 Configuration Tasks 27
1.8.4 Creating an IPv6 ACL 28
1.8.5 Applying an IPv6 ACL 29
1.9 Configuring an Expert Advanced ACL (ACL80) 30
1.9.1 Overview 30
1.9.2 Restrictions and Guidelines 30
1.9.3 Configuration Tasks 30
1.9.4 Creating an ACL80 31
1.9.5 Applying an ACL80 32
1.10 Configuring a Redirect ACL 33
1.10.1 Overview 33
1.10.2 Restrictions and Guidelines 33
1.10.3 Prerequisite 33
1.10.4 Procedure 33

1.11 Configuring a Global Security ACL 34
1.11.1 Overview 34
1.11.2 Restrictions and Guidelines 34
1.11.3 Prerequisite 34
1.11.4 Procedure 34
1.12 Configuring a Security Channel 35
1.12.1 Overview 35
1.12.2 Restrictions and Guidelines 35
1.12.3 Prerequisite 36
1.12.4 Procedure 36
1.13 Configuring the Fragmented Packet Matching Mode 36
1.13.1 Overview 36
1.13.2 Restrictions and Guidelines 36
1.13.3 Prerequisite 37
1.13.4 Procedure 37
1.14 Configuring an SVI Router ACL 37
1.14.1 Overview 37
1.14.2 Prerequisite 37
1.14.3 Procedure 37
1.15 Synchronizing All ACEs from Software to Hardware 38
1.15.1 Overview 38
1.15.2 Procedure 38
1.16 Monitoring 38
1.17 Examples 40

1.17.1 Configuring an IP Standard ACL....40
1.17.2 Configuring an IP Extended ACL....42
1.17.3 Configuring a MAC Extended ACL....47
1.17.4 Configuring an Expert Extended ACL....49
1.17.5 Configuring an IPv6 ACL....51
1.17.6 Configuring an ACL80....53
1.17.7 Configuring the ACL Packet Counting Function....55

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, attackers 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 attackers to access 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: Attackers 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 shorter idle time of user access. 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 networks
- 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 10, 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:

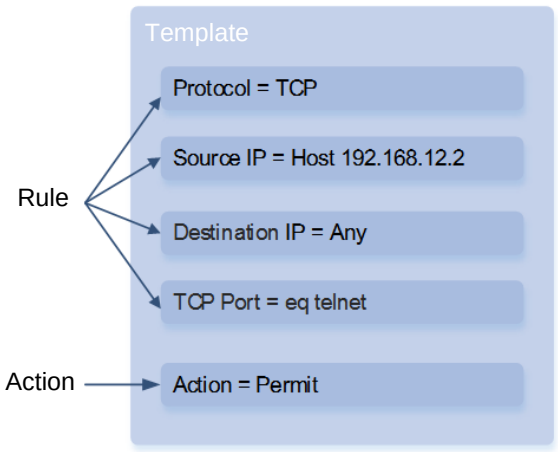
  ```
  10 permit tcp host 192.168.12.2 any eq telnet
  ```

  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.

- Action

  Action is specified in ACE. The actions include permit and deny. Permit means that the traffic matching the rules can pass, and deny means that the traffic matching the rules is rejected.

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.

Specification

- The outbound ACL acting on the physical port and L3 aggregation port (AP) only supports matching well-known packets (unicast and multicast), but does not support matching unknown unicast packets, that is, the outbound ACL configured on a port does not take effect for the unknown packets or broadcast packets.
- When the input ACL, IEEE 802.1x, global IP and MAC address binding, port security, and IP source guard are all configured, the permit and default deny ACEs do not take effect but other deny ACEs take effect normally.
- When the input ACL and QoS are configured, the permit ACE does not take effect, but other deny ACEs take effect normally; the default deny ACE takes effect after the QoS entry.
- If an ACE is added to an ACL after the ACL is applied to the inbound direction of multiple SVIs, and the device is restarted after the configuration is saved, the ACLs configured on several SVIs may fail to take effect due to the hardware capacity causes.

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

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.

Caution

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.

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

An 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.

Note

If an expert extended ACL rule does not specify IPv6 packets, that is, the Ethernet type field is not defined or the defined Ethernet type field is not 0x86dd, then the expert extended ACL does not 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 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.

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
```

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 fffffffffff 0
20 deny 00d0f8654321 fffffffffff 6
```

In ACE 10, the matching field content is 00d0f8123456, the matching field mask is fffffffffff, 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 fffffffffff, 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.

7. Redirect ACL

Redirect ACL enables a device to redirect the packets matching the rules to a specified port for forwarding. Or the device obtains and analyzes the packets in specified ports.

Redirect ACL binds an ACL on an input port and specifies an output port. When the input interface 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.

8. Global Security ACL

The global security ACL function can prevent the internal access to illegal websites or prevent viruses from entering the internal network of the enterprise. There are various virus packets in the network, and the identification characteristics of virus packets are the same or similar on each port. 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. 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.

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 priorities are global > interface. That is, the global security ACL is matched first, and then the security ACL of the interface is matched. The security ACL of the VLAN is independently matched.

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.

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.

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.

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.

Caution

- 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.
- 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.

Specification

- The log option can be configured for the IP ACL and IPv6 ACL rules only.

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.

Caution

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.

Specification

For IP ACL, MAC extended ACL, expert extended ACL, and IPv6 ACL, the packet matching counting function can be configured.

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 details about the time range configuration, see *Configuring Time Range* in **Configuration Guide** > **Device Management**.

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. In the default fragmented packet matching mode, 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 flag, 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.

Specification

- The fragmented packet matching mode can be switched only in the IP extended ACL and expert extended ACL.

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, Layer 3 Ethernet port, Layer 2 or Layer 3 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 Restrictions and Guidelines

- 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 ACLs with time-range options, you need to configure the time range. For details about time range configurations, see *Configuring Time Range* in **Configuration Guide** > **Device Management.**

1.3 Configuration Task Summary

ACL configuration tasks are as follows.

To configure an ACL, 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)
- Synchronizing All ACEs from Software to Hardware

1.4 Configuring an IP Standard ACL

1.4.1 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.

1.4.2 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.

1.4.3 Configuration Tasks

IP standard ACL configuration includes the following tasks:

(1) Creating an IP Standard ACL

(2) Applying an IP Standard ACL

1.4.4 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 IP standard ACL can contain no rules. 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.
- 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an IP standard ACL and rules. Please configure only one task.

- Create a numerically indexed IP standard ACL and rules.

access-list *acl-number* { **deny** | **permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

No IP standard ACL or rule is configured by default.

- Create a numerically indexed or named IP standard ACL and rules. Run the following commands in turn to create an IP standard ACL and rules.

  ip access-list standard { *acl-name* | *acl-number* }

  No IP standard ACL is configured by default.

  [*sequence-number*] { **deny | permit** } { *source-ipv4-address source-ipv4-wildcard* | **host** *source-ipv4-address* | **any** } [**time-range** *time-range-name*] [**log**]

  exit

  There is an ACL rule of deny type in an IP standard ACL by default.

(4) (Optional) Configure an update interval for packet matching logs.

ip access-list log-update interval *time-value*

The default update interval is 0 minutes. That is, no ACL matching log is output.

(5) (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** *text*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named IP standard ACL.

  ip access-list standard { *acl-name* | *acl-number* }

  list-remark *text*

  exit

No remark is configured for an ACL by default.

(6) (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** *text*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named IP standard ACL.

  ip access-list standard { *acl-name* | *acl-number* }

  [*sequence-number*] **remark** *text*

  exit

No remark is configured for ACL rules by default.

(7) (Optional) Enable the packet matching counting function of an IP standard ACL.

ip access-list counter { *acl-name* | *acl-number* }

The packet matching counting function of an IP standard ACL is disabled by default.

(8) (Optional) Configure a step for rule sequence numbers in the IP standard ACL.

ip access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

Both the start value and step of an IP standard ACL rule sequence numbers are **10** by default.

1.4.5 Applying an IP Standard ACL

1. Overview

Apply an IP standard ACL in the global configuration mode, interface configuration mode, SVI configuration mode, or VLAN configuration mode to make the IP standard ACL take effect.

2. Restrictions and Guidelines

- 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.
- 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.
- 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.
- After the ACL packet statistics collection is enabled, you can view the ACL configuration by running the **show access-lists** command, which includes the ACE configuration, ACE-based packet matching count, and ACL-based packet matching count. The ACL-based packet matching count only supports the statistics of packets denied by ACL.
- 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) (Optional) Apply an IP standard ACL globally.

ip access-group { *acl-name* | *acl-number* } **global** { **in** | **out** } [**control-plane** | **forward-control-plane** | **forward-plane**]

No IP standard ACL is applied globally by default.

(4) Enter the interface configuration mode, or VLAN configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan interface-*number*

- Enter the VLAN configuration mode.

  vlan *vlan-id*

(5) Apply an IP standard ACL.

ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

No IP standard ACL is applied to an interface by default.

1.5 Configuring an IP Extended ACL

1.5.1 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.

1.5.2 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.

1.5.3 Configuration Tasks

IP extended ACL configuration includes the following tasks:

(1) Creating an IP Extended ACL

(2) Applying an IP Extended ACL

1.5.4 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 IP extended ACL can contain no rules. 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.

- 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an IP extended ACL and its rules. Please configure only one task.

- Create a numerically indexed IP extended ACL and its rules.

  access-list *acl-number* { **deny** | **permit** } *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-range-name*] [**log**]

  No IP extended ACL or rule is configured by default.

- Create 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-name* | *acl-number* }

  No IP extended ACL is configured by default.

  [*sequence-number*] { **deny** | **permit** } *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-range-name*] [**log**]

  exit

  There is an ACL rule of deny type in an IP extended ACL by default.

(4) (Optional) Configure an update interval for packet matching logs.

ip access-list log-update interval *time-value*

The default update interval is 0 minutes. That is, no ACL matching log is output.

(5) (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 text*

- Run the following commands in turn to configure a remark for a numerically indexed or named IP extended ACL.

  ip access-list extended { *acl-name* | *acl-number* }

  list-remark *text*

  exit

No remark is configured for an ACL by default.

(6) (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** *text*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named ACL.

  ip access-list extended { *acl-name* | *acl-number* }

  [*sequence-number*] **remark** *text*

  exit

No remark is configured for ACL rules by default.

(7) (Optional) Enable the packet matching counting function of an IP extended ACL.

ip access-list counter { *acl-name* | *acl-number* }

The packet matching counting function of an IP extended ACL is disabled by default.

(8) (Optional) Configure the start value and the step for rule sequence numbers in the IP extended ACL.

ip access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

Both the start value and step of IP extended ACL rule sequence numbers are **10** by default.

1.5.5 Applying an IP Extended ACL

1. Overview

Apply an IP extended ACL in the global configuration mode, interface configuration mode, or SVI configuration mode to make the IP extended ACL take effect.

2. Restrictions and Guidelines

- 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.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- 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.

- After the ACL packet statistics collection is enabled, you can view the ACL configuration by running the **show access-lists** command, which includes the ACE configuration, ACE-based packet matching count, and ACL-based packet matching count. The ACL-based packet matching count only supports the statistics of packets denied by ACL.
- 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) (Optional) Apply an IP extended ACL globally.

ip access-group { *acl-name* | *acl-number* } **global** { **in** | **out** } [**control-plane** | **forward-control-plane** | **forward-plane**]

No IP extended ACL is applied globally by default.

(4) Enter the interface configuration mode, or VLAN configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan interface-*number*

- Enter the VLAN configuration mode.

  vlan *vlan-id*

(5) Apply an IP extended ACL.

ip access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only** | **forward-control-plane** | **forward-plane**]

No IP extended ACL is applied by default.

1.6 Configuring a MAC Extended ACL

1.6.1 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.

1.6.2 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.

1.6.3 Configuration Tasks

MAC extended ACL configuration includes the following tasks:

(1) Creating a MAC Extended ACL

(2) Applying a MAC Extended ACL

1.6.4 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 MAC extended ACL can contain no rules. 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.
- 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a MAC extended ACL and its rules. Please configure only one task.

- Create a numerically indexed MAC extended ACL and its rules.

  access-list *acl-number* { **deny** | **permit** } { *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-range-name*]

  No MAC extended ACL or rule is configured by default.

- Create 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-name* | *acl-number* }

  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.

  [*sequence-number*] { **deny** | **permit** } { *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-range-name*]

  exit

  There is an ACL rule of deny type in a MAC extended 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** *text*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named ACL.

  mac access-list extended { *acl-name* | *acl-number* }

  list-remark *text*

  exit

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** *text*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named ACL.

  mac access-list extended { *acl-name* | *acl-number* }

  [*sequence-number*] **remark** *text*

  exit

No remark is configured for ACL rules by default.

(6) (Optional) Enable the packet matching counting function of a MAC extended ACL.

mac access-list counter { *acl-name* | *acl-number* }

The packet matching counting function of a MAC extended ACL is disabled by default.

(7) (Optional) Configure the start value and the step for rule sequence numbers in the MAC extended ACL.

mac access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

Both the start value and step of MAC extended ACL rule sequence numbers are **10** by default.

1.6.5 Applying a MAC Extended ACL

1. Overview

Apply a MAC extended ACL in the global configuration mode, interface configuration mode, or SVI configuration mode to make the MAC ACL take effect.

2. Restrictions and Guidelines

- 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.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- 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.
- After the ACL packet statistics collection is enabled, you can view the ACL configuration by running the **show access-lists** command, which includes the ACE configuration, ACE-based packet matching count, and ACL-based packet matching count. The ACL-based packet matching count only supports the statistics of packets denied by ACL.
- 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) (Optional) Apply a MAC extended ACL globally.

mac access-group { *acl-name* | *acl-number* } **global** { **in** | **out** } [**control**-**plane** | **forward-control-plane** | **forward-plane**]

No MAC extended ACL is applied globally by default.

(4) Enter the interface configuration mode, or VLAN configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan interface-*number*

- Enter the VLAN configuration mode.

  vlan *vlan-id*

(5) Apply a MAC extended ACL.

mac access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only**| **forward-control-plane** | **forward-plane**]

No MAC extended ACL is applied by default.

1.7 Configuring an Expert Extended ACL

1.7.1 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.

1.7.2 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 configure an expert extended ACL 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.

1.7.3 Configuration Tasks

Expert extended ACL configuration includes the following tasks:

(1) Creating an Expert Extended ACL

(2) Applying an Expert Extended ACL

1.7.4 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 expert extended ACL can contain no rules. 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an expert extended ACL and its rules. Please configure only one task.

- Create a numerically indexed expert extended ACL and its rules.

  access-list *acl-number* { **deny** | **permit** } [*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-range-name*]

  No expert extended ACL or rule is configured by default.

- Create 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-name* | *acl-number* }

  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.

  [*sequence-number*] { **deny** | **permit** } **access-list** *acl-number* { **deny** | **permit** } [*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-range-name*]

  exit

  There is an ACL rule of deny type in an expert extended 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** *text*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named ACL.

  expert access-list extended { *acl-name* | *acl-number* }

  list-remark *text*

  exit

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*

- Run the following commands in turn to configure remarks for rules in the numerically indexed or named ACL.

  expert access-list extended { *acl-name* | *acl-number* }

  remark *text*

  exit

No remark is configured for ACL rules by default.

(6) (Optional) Enable statistics collection for expert ACL packet matching.

expert access-list counter { *acl-name* | *acl-number* }

(7) (Optional) Configure the start value and the step for rule sequence numbers in the expert extended ACL.

expert access-list resequence { *acl-name* | *acl-number* } *start-value step-value*

Both the start value and step of an expert ACL rule sequence numbers are **10** by default.

1.7.5 Applying an Expert Extended ACL

1. Overview

Apply an expert extended ACL in the global configuration mode, interface configuration mode, VLAN configuration mode, or SVI configuration mode to make the expert extended ACL take effect.

2. Restrictions and Guidelines

- 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.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- 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.
- After the ACL packet statistics collection is enabled, you can view the ACL configuration by running the **show access-lists** command, which includes the ACE configuration, ACE-based packet matching count, and ACL-based packet matching count. The ACL-based packet matching count only supports the statistics of packets denied by ACL.
- 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) (Optional) Apply an expert extended ACL globally.

expert access-group { *acl-name* | *acl-number* } **global** { **in** | **out** } [**control**-**plane** | **forward-control-plane** | **forward-plane**]

No expert extended ACL is applied globally by default.

(4) Enter the interface configuration mode, or VLAN configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan interface-*number*

- Enter the VLAN configuration mode.

  vlan *vlan-id*

(5) Apply an expert extended ACL to an interface.

expert access-group { *acl-name* | *acl-number* } { **in** | **out** } [**control-plane** | **counter-only**| **forward-control**-**plane** | **forward-plane**]

No expert extended ACL is applied to an interface by default.

1.8 Configuring an IPv6 ACL

1.8.1 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.

1.8.2 Restrictions and Guidelines

- To control IPv6 users' access to network resources, configure an IPv6 ACL.
- You can configure an IPv6 ACL on an access, convergence, or core device based on the distribution of users. The IPv6 ACL takes effect only on the local device, but does not affect other devices in the network.

1.8.3 Configuration Tasks

IPv6 ACL configuration includes the following tasks:

(1) Creating an IPv6 ACL

(2) Applying an IPv6 ACL

1.8.4 Creating an IPv6 ACL

1. Overview

This section describes how to create an IPv6 ACL and configure its rules.

2. Restrictions and Guidelines

- You cannot specify the name of an IPv6 ACL but its number.
- An IPv6 ACL can contain no rules. When no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the IPv6 ACL to prohibit all IPv6 packets except ND packets from entering the device.
- 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.

[*sequence-number*] { **deny** | **permit** } [*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** }] [**cos** *cos-value* [**inner** *cos-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**] * [**time-range** *time-range-name*] [**log**] [VID [*vlan-id*] [**inner** *vlan-id*]]

(5) (Optional) Configure a remark for the ACL.

list-remark *text*

No remark is configured for an ACL by default.

(6) (Optional) Configure remarks for ACL rules.

[*sequence-number*] **remark** *text*

No remark is configured for ACL rules by default.

(7) Exit the global configuration mode.

exit

(8) (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.

(9) (Optional) Configure the device to display match statistics for IPv6 ACLs.

ipv6 access-list counter *acl-name*

The device is disabled from displaying match statistics for IPv6 ACLs by default.

(10) (Optional) Configure the start value and the step for rule sequence numbers in the IPv6 extended ACL.

ipv6 access-list resequence *acl-name start-value step-value*

Both the start value and step of an IPv6 ACL rule sequence numbers are **10** by default.

1.8.5 Applying an IPv6 ACL

1. Overview

Apply an IPv6 ACL in the global configuration mode, interface configuration mode, or SVI configuration mode to make the IPv6 ACL take effect.

2. Restrictions and Guidelines

- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- 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.
- After the ACL packet statistics collection is enabled, you can view the ACL configuration by running the **show access-lists** command, which includes the ACE configuration, ACE-based packet matching count, and ACL-based packet matching count. The ACL-based packet matching count only supports the statistics of packets denied by ACL.
- 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, or VLAN configuration mode.

- Enter the Layer 2 interface configuration mode.

  interface *interface-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the VLAN interface configuration mode.

  interface vlan *vlan-id*

- Enter the VLAN configuration mode.

  vlan *vlan-id*

(4) Apply an IPv6 ACL.

ipv6 traffic-filter *acl-name* { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

No IPv6 ACL is applied to an interface by default.

1.9 Configuring an Expert Advanced ACL (ACL80)

1.9.1 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 expert advanced ACL (ACL80) to define the packet fields to be matched.

1.9.2 Restrictions and Guidelines

- You can configure an ACL80 on an access, convergence, or core device based on the distribution of users. The ACL80 takes effect only on the configured device, but does not affect other devices in the network.

1.9.3 Configuration Tasks

The ACL80 configuration includes the following tasks:

(1) Creating an ACL80

(2) Applying an ACL80

1.9.4 Creating an ACL80

1. Overview

This section describes how to create an ACL80 and configure its rules.

2. Restrictions and Guidelines

- An ACL80 supports matching Ethernet II packets, IEEE 802.2 LLC SNAP packets, and IEEE 802.2 packets. If the values of the DSAP field to the Control field to be matched are AAAA03, IEEE 802.2 SNAP packets are matched. If the values of the DSAP field to the Control field to be matched are E0E003, IEEE 802.2 LLC packets are matched. If an ACL80 tries to match Ethernet II packets, you cannot set the values of the DSAP field to the Control field.
- Due to hardware, currently ACL80 cannot implement random byte matching for the first 80 bytes of packets, but only supports matching the fields 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 in packets.
- When an ACL80 matches 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, run the **permit 0800 FFFF 24 C0A80102 FFFFFFFF 38** command.
- An ACL80 can contain no rules. 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.
- When an ACL is used to redirect Layer 2 broadcast packets to an aggregate interface, if the aggregate interface has member interfaces across chips (including member interfaces across devices in VSU mode) and the load balancing mode is **src-dst-ip**, some traffic may fail to be forwarded through members of the aggregate interface, resulting in packet loss. If you need to redirect Layer 2 broadcast packets to an aggregate interface, use either of the following methods to avoid packet loss:
  - Change the load balancing mode of the aggregate interface to MAC-based load balancing.
  - Configure member interfaces of an aggregate interface on the same chip or the same device.

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.

[*sequence-number*] { **deny** | **permit** } *hex hex-mask offset*

No expert advanced ACL is configured.

(5) (Optional) Configure a remark for the ACL.

list-remark *text*

No remark is configured for an ACL by default.

(6) (Optional) Configure remarks for ACL rules.

[*sequence-number*] **remark** *text*

No remark is configured for ACL rules by default.

1.9.5 Applying an ACL80

1. Overview

Apply an ACL80 in the global configuration mode, interface configuration mode, SVI configuration mode, VLAN configuration mode to make the ACL80 take effect.

2. Restrictions and Guidelines

- 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, or VLAN configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan interface-*number*

- Enter the VLAN configuration mode.

  vlan *vlan-id*

(4) Apply an expert advanced ACL.

expert access-group { *acl-name* | *acl-number* } { **in** | **out** }

No expert advanced ACL is applied by default.

1.10 Configuring a Redirect ACL

1.10.1 Overview

This section describes how to configure the ACL-based redirection 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.

1.10.2 Restrictions and Guidelines

- You can configure the ACL-based redirection 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 L2 Ethernet interface and an L2 aggregate interface 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.
- If no rule is configured in an ACL, the ACL-based redirection function is unavailable.

1.10.3 Prerequisite

You must configure an ACL first to enable the ACL-based redirection function.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

(4) Configure a redirect ACL on an interface.

redirect destination interface *interface-type interface-number* **acl** { *acl-name* | *acl-number* } **in**

No redirect ACL is configured on a port by default.

1.11 Configuring a Global Security ACL

1.11.1 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, you can configure excluded ports of the global security ACL to permit some special departments in an enterprise to access some external websites.

1.11.2 Restrictions and Guidelines

- If no rule is configured in an ACL, the global security ACL function is unavailable.
- Since the global security ACL is mainly used for virus filtering, among the ACEs in a global security ACL, only the deny ACEs take effect, and the permit ACEs do take effect.
- Different from a security ACL applied to a port, a global security ACL has no default rule of denying all entries, that is, the packets not matching the rules in a global security ACL can pass through.
- Global security ACLs can be associated only with IP standard ACLs, IP extended ACLs, MAC extended ACLs, and expert extended ACLs.
- A global security ACL takes effect on both Layer 2 and Layer 3 interfaces.
- You can disable the global security ACL function on a physical port, Layer 2 link aggregation or Layer 3 link aggregation. You cannot disable the global security ACL function on a member port of a link aggregation.
- You can configure a global security ACL 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.
- Disable the global security ACL function to forbid configuring global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

1.11.3 Prerequisite

You must configure an ACL first to enable the global security ACL function.

1.11.4 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 enabled by default.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.
  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.
  interface aggregateport *interface-number*

No global security ACL is configured by default.

(5) (Optional) Enable a global security ACL on the port.

global access-group

A port is an excluded port of a global security ACL by default.

(6) (Optional) Enable a global IP security ACL on the port.

global ip access-group

A port is an excluded port of a global IP security ACL by default.

1.12 Configuring a Security Channel

1.12.1 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.

1.12.2 Restrictions and Guidelines

- If no rule is configured in an ACL, the security channel function is unavailable.
- The deny action in an ACL applied to 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 a 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 a security channel are used, the security channel does not take effect.
- You cannot set an IPv6 ACL as a security channel.
- 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. You must configure one of the two tasks.
- 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.
- 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.

1.12.3 Prerequisite

You must configure an ACL first to enable the global security ACL function.

1.12.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a global security channel.

security global access-group { *acl-name* | *acl-number* }

No global security channel is configured by default.

Choose either global security channel or interface security channel to configure.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(5) (Optional) Configure a security channel for a port.

security access-group { *acl-name* | *acl-number* }

No security channel is configured on a port by default.

Choose either global security channel or interface security channel to configure.

(6) (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 by default.

1.13 Configuring the Fragmented Packet Matching Mode

1.13.1 Overview

This function can be configured to enable ACL to control fragmented packets more finely.

1.13.2 Restrictions and Guidelines

- When you switch the fragmented packet matching mode, the ACL fails for a short period of time.

- In a new fragmented packet matching mode, if an ACL rule does not carry a fragment flag and the matching action is permit, such an ACL rule occupies more hardware entry resources, and, in extreme cases, halves the capacity of hardware policy entries. If such an ACE is configured to filter established TCP packets, more hardware policy entry resources will be occupied.
- In a new fragmented packet matching mode, if an ACL rule does not carry a fragment flag and needs to match the Layer 4 information of packets, when the matching action is permit, the ACL rule checks the Layer 3 and Layer 4 information of the first fragment, and checks only the Layer 3 information of the non-first fragments.
- In a new fragmented packet matching mode, if an ACL rule carries a fragment flag, no matter whether the matching action of the ACL rule is permit or deny, the ACL rule checks only the non-first fragments.

1.13.3 Prerequisite

You must configure an ACL first to switch the fragmented packet matching mode.

1.13.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a new fragmented packet matching mode. Configure only one of the following tasks.

- Configure a new fragmented packet matching mode of an IP ACL.

  ip access-list new-fragment-mode { *acl-name* | *acl-number* }

  No new fragmented packet matching mode is configured for an IP ACL by default.

- Configure a new fragmented packet matching mode of an expert extended ACL.

  expert access-list new-fragment-mode { *acl-name* | *acl-number* }

  No new fragmented packet matching mode is configured for an expert extended ACL by default.

1.14 Configuring an SVI Router ACL

1.14.1 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.

1.14.2 Prerequisite

To implement this function, first configure an ACL.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an SVI router ACL.

svi router-acls enable

1.15 Synchronizing All ACEs from Software to Hardware

1.15.1 Overview

When the entry capacity of the device software is greater than that supported by the hardware, no ACE can be added. When the entry capacity of the device software drops below that supported by the hardware, the ACEs that fail to be added before will not be added again. This command can be used to refresh the configuration to trigger the re-adding of ACEs, thus synchronizing ACEs from software to hardware.

1.15.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Synchronize all ACEs from software to hardware.

acl ref synchronize all

1.16 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

During device operation, running the **clear** command may cause service interruption due to key information loss.

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

Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 1-5 ACL Monitoring

Command	Purpose
show access-lists [*acl-name* | *acl-number*] [**summary**]	Displays a basic ACL.

Command	Purpose
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 arp access-group [**interface** *interface-type interface-number*]	Displays the configuration of an ARP extended ACL applied to a port.
show acl res [**dev** *dev-number* [**slot** *slot-number*]]	Displays information about all ternary content-addressable memory (TCAMs) or a specified TCAM.
show acl capability [**more**]	Displays device capability.
show svi router-acls state	Checks whether an ACL applied to an SVI takes effect on L2 and L packets.
show acl res detail [**dev** *dev-num* [**slot** *slot-num*]]	Displays usage details about all TCAMs or a specified TCAM.
clear acl res	Clears historical peak information of TCAM resource usage.
clear counters access-list [*acl-name* | *acl-number*]	Clears the number of packets matching an ACE.
clear access-list counters [*acl-name* | *acl-number*]	Clears the number of packets matching an ACL 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.

1.17 Examples

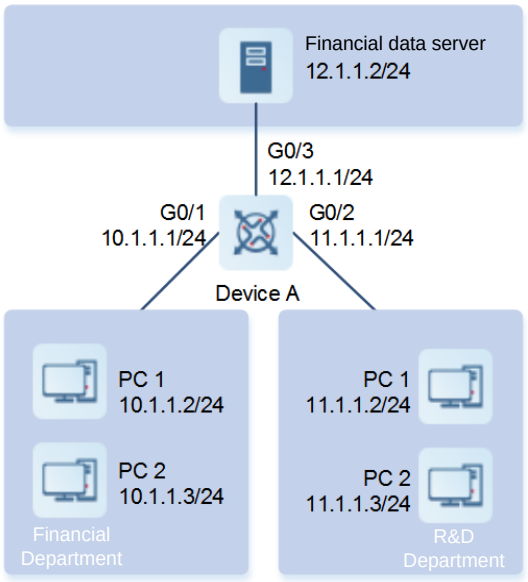
1.17.1 Configuring an IP Standard ACL

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 Configuring IP Standard ACL



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
!
```

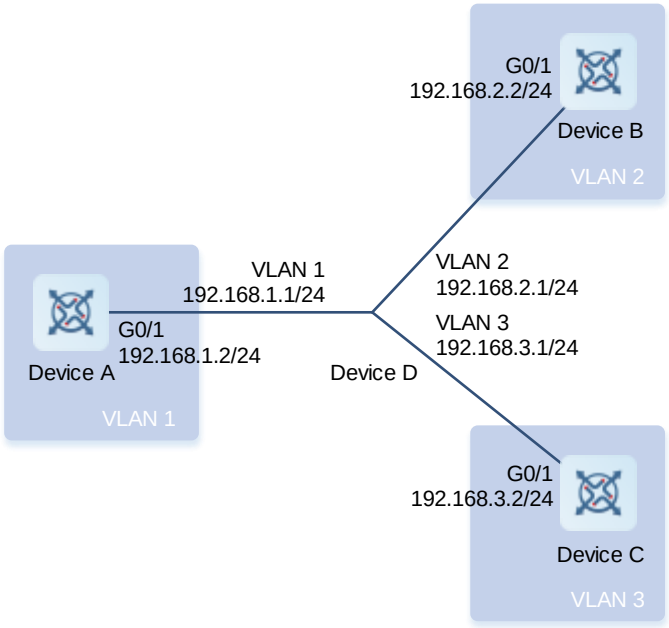
1.17.2 Configuring an IP Extended ACL

1. Requirements

Device A (VLAN 1), device B (VLAN 2), and device C (VLAN 3) are directly connected to device 4, 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 Configuring IP Extended ACL Application Scenario



3. Notes

- On device D, 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 device 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 device A, apply the IP extended ACL to VLAN 1 interface, VLAN 2 interface, and VLAN 3 interface. On device C, apply the IP extended ACL to interface GigabitEthernet 0/1 that is connected to Device D.

4. Procedure

(1) Configure IP addresses for all the device ports (omitted).

(2) Configure an IP extended ACL and add access rules.

On device D, configure an IP extended ACL and add access rules.

```
DeviceD> enable
DeviceD# configure terminal
```

```
DeviceD(config)# ip access-list extended inter_vlan_access1
DeviceD(config-ext-nacl)# deny udp any eq bootps any eq bootpc
DeviceD(config-ext-nacl)# deny udp any eq bootpc any eq bootps
DeviceD(config-ext-nacl)# remark //Deny DHCP packets.
DeviceD(config-ext-nacl)# permit ip any any
DeviceD(config-ext-nacl)# remark //Permit the communication using other
packets.
DeviceD(config-ext-nacl)# exit
DeviceD(config)# ip access-list extended inter_vlan_access2
DeviceD(config-ext-nacl)# deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
DeviceD(config-ext-nacl)# remark //Deny the mutual access between VLAN 2 and
VLAN 3.
DeviceD(config-ext-nacl)# deny udp any eq bootpc any eq bootps
DeviceD(config-ext-nacl)# deny udp any eq bootps any eq bootpc
DeviceD(config-ext-nacl)# remark //Deny DHCP packets.
DeviceD(config-ext-nacl)# permit ip any any
DeviceD(config-ext-nacl)# remark //Permit the communication using other
packets.
DeviceD(config-ext-nacl)# exit
DeviceD(config)# ip access-list extended inter_vlan_access3
DeviceD(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
DeviceD(config-ext-nacl)# remark //Deny the mutual access between VLAN 2 and
VLAN 3.
DeviceD(config-ext-nacl)# permit ip any any
DeviceD(config-ext-nacl)# remark //Permit the communication using other
packets.
DeviceD(config-ext-nacl)# exit
```

On device C, configure an IP extended ACL and add access rules.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# ip access-list extended access_deny
DeviceC(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 eq telnet any eq
telnet
DeviceC(config-ext-nacl)# remark //Deny VLAN 1 access to VLAN 3 through
telnet.
DeviceC(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 eq 22 any eq 22
DeviceC(config-ext-nacl)# remark //Deny VLAN 1 access to VLAN 3 through SSH.
DeviceC(config-ext-nacl)# permit any any
DeviceC(config-ext-nacl)# remark permit other packets to pass
DeviceC(config-ext-nacl)# exit
```

(3) Apply the IP extended ACLs.

On device D, apply the IP extended ACL to the corresponding ports.

```
DeviceD(config)# interface vlan 1
DeviceD(config-if-VLAN 1)# ip access-group inter_vlan_access1 in
```

```
DeviceD(config-if-VLAN 1)# exit
DeviceD(config)# interface vlan 2
DeviceD(config-if-VLAN 2)# ip access-group inter_vlan_access2 in
DeviceD(config-if-VLAN 2)# exit
DeviceD(config)# interface vlan 3
DeviceD(config-if-VLAN 3)# ip access-group inter_vlan_access3 in
DeviceD(config-if-VLAN 3)# exit
```

On device C, apply the IP extended ACL to the line connected to the switch.

```
DeviceC(config)# line vty 0
DeviceC(config-line)# access-class access_deny in
DeviceC(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.

```
DeviceA# 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
DeviceA#
DeviceA# 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.

```
DeviceB# 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.

```
DeviceA# 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
DeviceA#
DeviceA# telnet 192.168.3.2
Trying 192.168.3.2, 23...
% Destination unreachable; gateway or host down
```

6. Configuration Files

- Device D configuration file

```
hostname DeviceD
!
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_DeviceA
!
interface GigabitEthernet 1/1
 switchport access vlan 2
 description link_to_DeviceB
!
interface GigabitEthernet 1/2
 switchport access vlan 3
 description link_to_DeviceC
!
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
!
```

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
!
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
```

- Device C configuration file

```
hostname DeviceC
!
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.
30 permit ip any any
remake permit other packets to pass
!
interface GigabitEthernet 0/1
 ip address 192.168.3.2 255.255.255.0
!
line vty 0
 access-class access_deny in
 login
 password 7 $10$184$HItkSIIBDRBo$
!
```

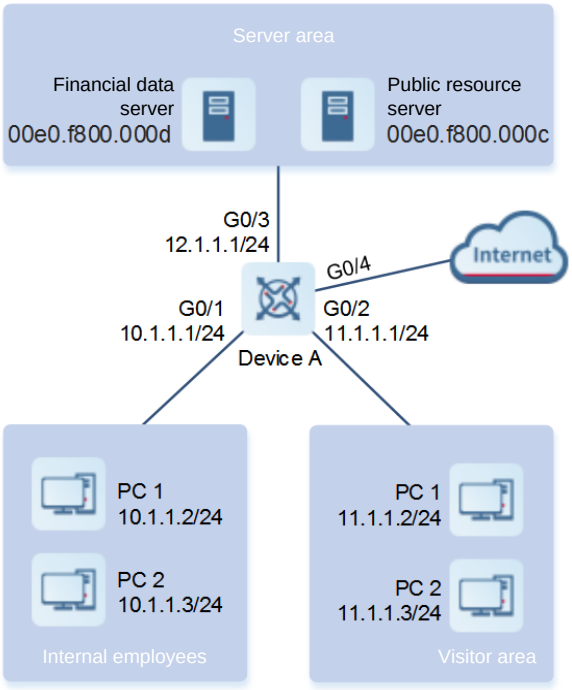
1.17.3 Configuring a MAC Extended ACL

1. Requirements

A MAC extended ACL needs to be configured to restrict the resources accessible to visitors.

2. Topology

Figure 1-5 Topology of Configuring MAC Extended ACL



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
!
```

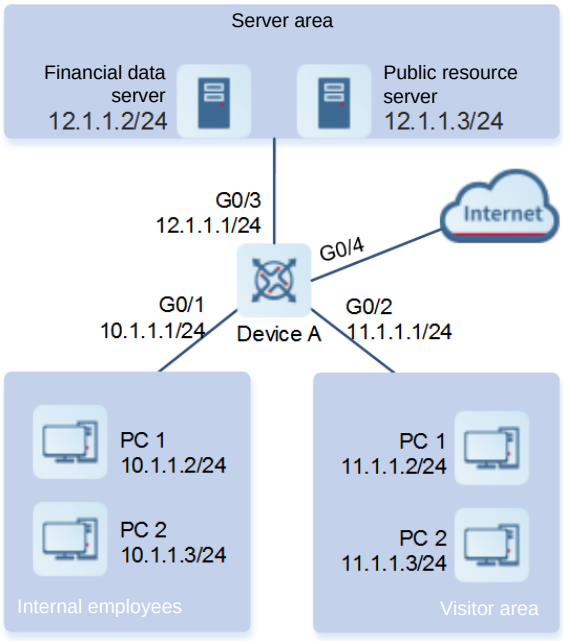
1.17.4 Configuring an Expert Extended ACL

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 and Internet.

2. Topology

Figure 1-6 Topology of Configuring Expert Extended ACL



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# 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# 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
!
```

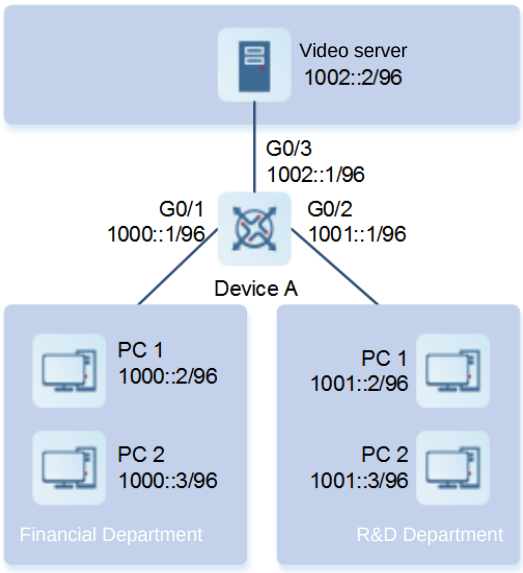
1.17.5 Configuring an IPv6 ACL

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 Configuring IPv6 ACL



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
!
```

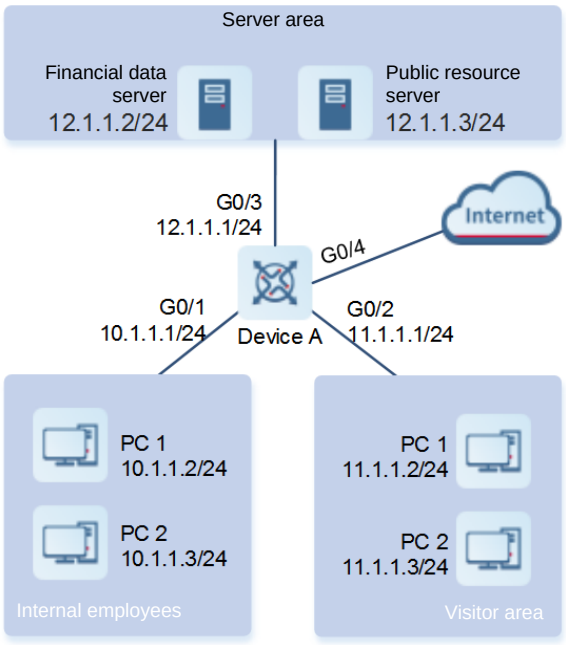
1.17.6 Configuring an ACL80

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 and Internet.

2. Topology

Figure 1-8 Topology of Configuring ACL80



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
!
```

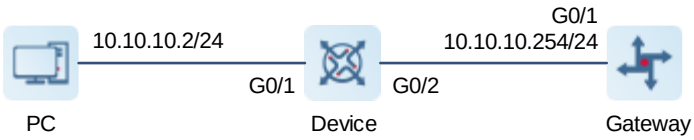
1.17.7 Configuring the ACL Packet Counting Function

1. Requirements

When you apply an ACL, you can configure the **counter-only** option to count the packets with some characteristics. The following example counts the ICMP packets discarded by the PC ping gateway and locate the discarded packets.

2. Topology

Figure 1-9 ACL Packet Statistics Topology



3. Notes

- Apply ACLs to both inbound and outbound directions of G0/1 and G0/2 on the device. You need to configure four ACLs on the device to match the ICMP packets from the PC to the gateway and from the gateway to the PC.
- Apply ACLs to both inbound and outbound directions of G0/1 on the gateway. You need to configure two ACLs on the gateway to match the ICMP packets from the PC to the gateway and from the gateway to the PC.
- Configure the **counter-only** option when you apply an ACL.
- The function only counts the packets matching the permit rule in the ACL and does not count those matching the deny rule.

4. Procedure

(1) Configure an ACL.

Configure four ACLs on the device to match the ICMP packets from the PC to the gateway and from the gateway to the PC.

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extend 100
Device(config-ext-nacl)# permit icmp host 10.10.10.2 host 10.10.10.254
Device(config-ext-nacl)# exit
Device(config)# ip access-list extend 101
```

```
Device(config-ext-nacl)# permit icmp host 10.10.10.254 host 10.10.10.2
Device(config-ext-nacl)# exit
Device(config)# ip access-list extend 102
Device(config-ext-nacl)# permit icmp host 10.10.10.2 host 10.10.10.254
Device(config-ext-nacl)# exit
Device(config)# ip access-list extend 103
Device(config-ext-nacl)# permit icmp host 10.10.10.254 host 10.10.10.2
Device(config-ext-nacl)# exit
```

Configure two ACLs on the gateway to match the ICMP packets from the PC to the gateway and from the gateway to the PC.

```
Gateway> enable
Gateway #configure terminal
Gateway(config)# ip access-list extend 100
Gateway(config-ext-nacl)# permit icmp host 10.10.10.2 host 10.10.10.254
Gateway(config-ext-nacl)# exit
Gateway(config)# ip access-list extend 101
Gateway(config-ext-nacl)# permit icmp host 10.10.10.254 host 10.10.10.2
Gateway(config-ext-nacl)# exit
```

(2) Apply ACLs.

Apply ACLs to both inbound and outbound directions of the interconnected interface, G0/1, on the gateway and the device.

```
DeviceA(config)# interface VLAN 10
DeviceA(config-if-VLAN 10)# ip address 172.16.1.3 255.255.255.0
DeviceA(config-if-VLAN 10)# vrrp 10 ip 172.16.1.1
DeviceA(config-if-VLAN 10)# vrrp 10 priority 120
DeviceA(config-if-VLAN 10)# exit
DeviceA(config)# interface VLAN 20
DeviceA(config-if-VLAN 20)# ip address 172.31.1.4 255.255.255.0
DeviceA(config-if-VLAN 20)# vrrp 20 ip 172.31.1.1
```

Apply ACLs to both inbound and outbound directions of the interconnected interface, G0/2, on the gateway and the device.

```
Device# configure terminal
Device(config)# interface gigabitEthernet 0/2
Device(config-if-GigabitEthernet 0/2)# ip access-group 103 in counter-only
Device(config-if-GigabitEthernet 0/2)# ip access-group 102 out counter-only
Device(config-if-GigabitEthernet 0/2)# exit
```

Apply ACLs to both inbound and outbound directions of the interconnected interface, G0/1, on the device and the PC.

```
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip access-group 100 in counter-only
Device(config-if-GigabitEthernet 0/1)# ip access-group 101 out counter-only
Device(config-if-GigabitEthernet 0/1)# exit
```

5. Verification

Send a total of 15 ICMP packets three times from the PC ping gateway address, 10.10.10.254. Display the count of ICMP packets on the device and the gateway respectively. Display the count of ICMP packets on the device.

```
Device# show access-lists
ip access-list extended 100
   10 permit ip host 10.10.10.2 host 10.10.10.254 (15 matches)
ip access-list extended 101
   10 permit ip host 10.10.10.254 host 10.10.10.2 (10 matches)
ip access-list extended 102
   10 permit ip host 10.10.10.2 host 10.10.10.254 (15 matches)
ip access-list extended 103
   10 permit ip host 10.10.10.254 host 10.10.10.2 (10 matches)
```

Display the count of ICMP packets on the gateway.

```
Gateway# show access-lists
ip access-list extended 100
   10 permit ip host 10.10.10.2 host 10.10.10.254 (15 matches)
ip access-list extended 101
   10 permit ip host 10.10.10.254 host 10.10.10.2 (15 matches)
```

Analyze the count of ICMP packets and locate the discarded packets

15 packets are received in the inbound direction of the interconnected interface, G0/1, of the device and the PC. (ACL 100 is applied to the device.)

15 packets are sent from the outbound direction of the interconnected interface, G0/2, of the device and the gateway. (ACL 102 is applied to the device.)

15 packets are received in the inbound direction of the interconnected interface, G0/1, of the gateway and the device. (ACL 100 is applied to the gateway.)

15 packets are sent from the outbound direction of the interconnected interface, G0/1, of the gateway and the device. (ACL 101 is applied to the gateway.)

10 packets are received in the inbound direction of the interconnected interface, G0/2, of the device and the gateway. (ACL 103 is applied to the device.)

The packets were discarded in the link between the device and the gateway.

6. Configuration Files

- Device configuration file

```
hostname Device
!
ip access-list extended 100
 10 permit icmp host 10.10.10.2 host 10.10.10.254
!
ip access-list extended 101
 10 permit icmp host 10.10.10.254 host 10.10.10.2
!
ip access-list extended 102
```

```
 10 permit icmp host 10.10.10.2 host 10.10.10.254
!
ip access-list extended 103
 10 permit icmp host 10.10.10.254 host 10.10.10.2
!
interface GigabitEthernet 0/1
 ip access-group 100 in counter-only
 ip access-group 101 out counter-only
!
interface GigabitEthernet 0/2
 ip access-group 103 in counter-only
 ip access-group 104 out counter-only
!
```

- Gateway configuration file

```
hostname Gateway
!
ip access-list extended 100
 10 permit icmp host 10.10.10.2 host 10.10.10.254
!
ip access-list extended 101
 10 permit icmp host 10.10.10.254 host 10.10.10.2
!
interface GigabitEthernet 0/1
 ip access-group 100 in counter-only
 ip access-group 101 out counter-only
 ip address 10.10.10.254 255.255.255.0
!
```

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
1.2.1 Overview 8
1.2.2 Configuration Tasks 8
1.2.3 Configuring a Class 8
1.2.4 Configuring a Policy 9
1.2.5 Applying a Policy 10
1.2.6 Configuring a Logical Interface Group 10
1.3 Configuring Priority Mapping 12
1.3.1 Overview 12
1.3.2 Configuration Tasks 12
1.3.3 Configuring the Trust Mode 12
1.3.4 Configuring Mappings 13
1.4 Configuring the Interface Rate Limit 14
1.4.1 Overview 14
1.4.2 Procedure 14
1.5 Configuring Congestion Management 14
1.5.1 Overview 14
1.5.2 Configuration Tasks 14

1.5.3 Configuring the CoS-to-Queue Mappings 15
1.5.4 Configuring the Scheduling Policy and Round Robin Weights for Global Output Queues 15
1.5.5 Configuring the Scheduling Policy and Round Robin Weights for Output Queues on an Interface 16
1.5.6 Configuring Bandwidth for a Queue 17
1.6 Configuring the QoS Global Policy 18
1.6.1 Overview 18
1.6.2 Procedure 18
1.7 Monitoring 18
1.8 Configuration Examples 20
1.8.1 Configuring the Interface Rate Limit and Priority Re-marking 20
1.8.2 Configuring Queue Scheduling and Congestion Avoidance 23

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

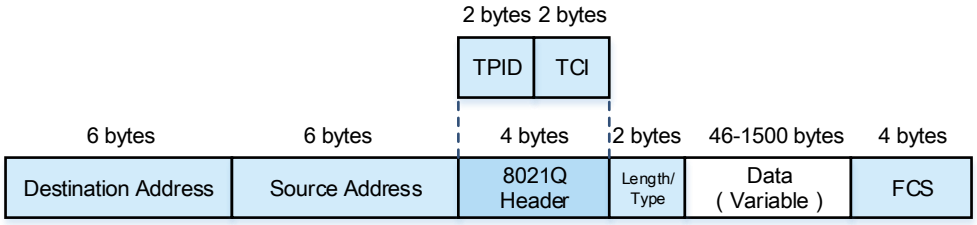
  The differentiated services (DiffServ) model classifies all packets transmitted on a network into different types. The classification information related to QoS priority marking is recorded in some fields of L2 or L3 packets, for example, the PRI field of IEEE 802.1Q frames, type of service (ToS) field of IPv4 packets, 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

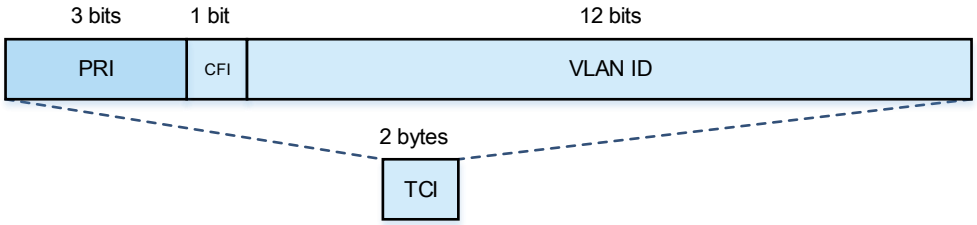
  The PRI field of IEEE 802.1Q frames (namely, the IEEE 802.1p priority) is located in the header of an L2 packet containing an IEEE 802.1Q tag header, as shown in Figure 1-1.

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

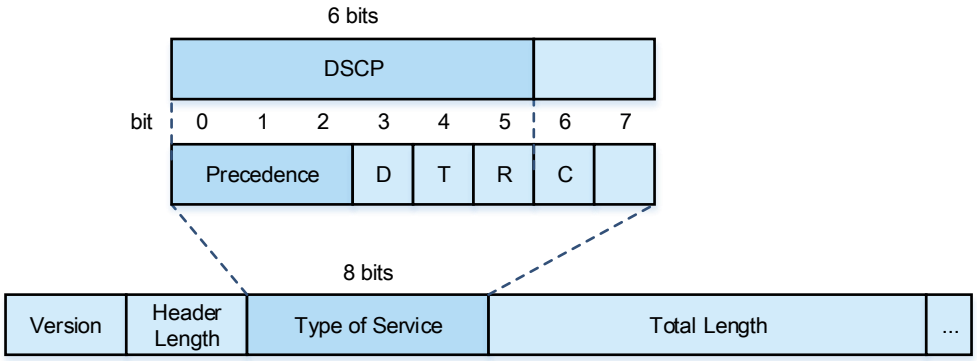


The PRI field represents eight priorities for packet transmission, and the priority values from high to low are 7, 6, ..., 1, and 0. The IEEE 802.1p priority is applicable to scenarios where L3 headers do not need to be analyzed and QoS needs to be implemented only at L2.

- 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



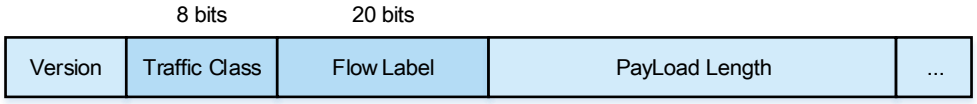
The ToS field contains eight bits, of which the first three bits are the IP PRE (precedence) field and represent eight priorities for packet transmission, with the priority values from high to low being 7, 6, ..., 1, and 0.

RFC 2474 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 1-4.

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, 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

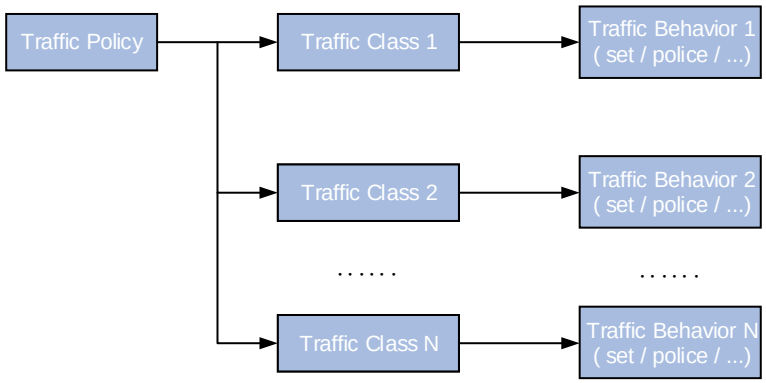
  Complex traffic classification classifies packets based on the priorities carried in packets or by identifying packets meeting certain characteristics according to access control list (ACL) rules.

  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 (Traffic Class) comprises the class name and class rule. A class defines the matching rules of traffic classification to classify packets.
  - A traffic (Traffic Behavior) 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 (Traffic 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.

The policy-based binding between multiple traffic classes and behaviors is as shown in Figure 1-6.

Figure 1-5 Policy-Based Binding Between Multiple Traffic Classes and Behaviors



- 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.

Interface Trust Mode	Priority Mapping
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.
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. Before sending a packet, check whether there is a packet to be sent in a high-priority queue. If there is, send it. If not, check whether there is a packet to be sent in the next-level queue, and so on.

  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 the DRR scheduling is implemented based on the packet byte size 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.

Like unicast queues, multicast queues can also be configured with priority mapping and scheduling algorithms. Currently multicast queues support the following scheduling algorithms: SP, WRR, and SP+WRR.

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 a Class
  - Configuring a Policy
  - Applying a Policy
  - (Optical) Configuring a Logical Interface Group
- Configuring Priority Mapping
  - Configuring the Trust Mode
  - Configuring Mappings
- Configuring the Interface Rate Limit
- Configuring Congestion Management
  - Configuring the CoS-to-Queue Mappings
  - Configuring the Scheduling Policy and Round Robin Weights for Global Output Queues
  - Configuring the Scheduling Policy and Round Robin Weights for Output Queues on an Interface
  - Configuring Bandwidth for a Queue
  - Configuring the QoS Global Policy
- Configuring Traffic Classification

1.2.1 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.

1.2.2 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

1.2.3 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-name* | *acl-number* }

  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 *precedence-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.

1.2.4 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. To configure other traffic behaviors, you must delete this traffic behavior.

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, DSCP values.

  set { **cos** *cos-value* | **ip dscp** *dscp-value* }

- Bind the class to the traffic behavior of limiting the bandwidth and processing packets beyond the limit.

  police *rate-value burst-value* [**exceed-action drop**]

(6) Bind the class to the traffic behavior of discarding packets.

drop

A class is not bound to any traffic behavior by default.

1.2.5 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 a Layer 2 Ethernet interface, a Layer 3 Ethernet interface and a Layer 3 link aggregation. Certain products support the application of policies to switch virtual interfaces (SVIs).
- 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.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Apply a policy in global configuration mode.

service-**policy input** *policy-map-name*

No policy is applied globally by default.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *vlan-id*

(5) Apply a policy in interface configuration mode.

service-**policy input** *policy-map-name*

No policy is applied to an interface by default.

1.2.6 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

virtual-group *virtual-group-number*

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

(5) Add an interface to a logical interface group.

virtual-group *virtual-group-number*

An interface is not added to any logical interface group by default.

(6) Return to the global configuration mode.

exit

(7) Enter the logical interface group configuration mode.

virtual-group *virtual-group-number*

(8) Apply a policy to the logical interface group.

service-policy input *policy-map-name*

1.3 Configuring Priority Mapping

1.3.1 Overview

Priority mapping can be implemented based on the trust mode configured for an interface.

1.3.2 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

1.3.3 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 interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregateport interface configuration mode.

  interface aggregateport *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**.

1.3.4 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.

1.4 Configuring the Interface Rate Limit

1.4.1 Overview

This section describes how to configure traffic limit for an interface.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregateport interface configuration mode.

  interface aggregateport *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 *rate-value burst-value*

- Configure the rate limit for the traffic in the output direction of an interface.

  rate-limit output *rate-value burst-value*

No traffic limit is configured for an interface by default.

1.5 Configuring Congestion Management

1.5.1 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.

1.5.2 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 Global Output Queues
- Configuring the Scheduling Policy and Round Robin Weights for Output Queues on an Interface

- Configuring Bandwidth for a Queue

1.5.3 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-value* &<1-8>

The CoS values 0 to 7 are mapped to the queues 1 to 8 respectively by default.

1.5.4 Configuring the Scheduling Policy and Round Robin Weights for Global Output Queues

1. Overview

This section describes how to configure the scheduling policy and round robin weights for output queues.

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.
- 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.
- Run the **priority-queue out** command to set the scheduling policy of output queues to SP. The effect is the

same as that of the **mls qos scheduler sp** command. Run the **show running-config** command. The command is displayed as **mls qos scheduler sp** instead of **priority-queue out**.

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.

- 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**.

- Set the scheduling policy to SP scheduling.

  priority-queue

  The default scheduling policy of output queues is **WRR**.

- Set the scheduling policy to SP scheduling.

  priority-queue out

  The default scheduling policy of output queues is **WRR.**

(4) Configure the round robin weight for the scheduling policy of global output queues.

{ **drr-queue** | **wfq-queue** | **wrr-queue** } **bandwidth** *weight-value-list*

The default round robin weight ratio of global queues is **1:1:1:1:1:1:1:1**.

1.5.5 Configuring the Scheduling Policy and Round Robin Weights for Output Queues on an Interface

1. Overview

This section describes how to configure the scheduling policy and round robin weights for output queues.

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.
- 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.
- Run the **qos mc-queue scheduler weight** command to configure the round robin weight for the scheduling policy of multicast output queues. A higher weight means longer output time.

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

(4) Configure the scheduling policy for interface output queues.

mls qos scheduler { **drr** | **rr** | **sp** | **wfq** | **wrr** }

No scheduling policy is configured on an interface by default.

(5) Configure the round robin weight for the scheduling policy of interface output queues.

{ **drr**-**queue** | **wfq**-**queue** | **wrr**-**queue** } **bandwidth** *weight-value-list*

The default round robin weight ratio of interface queues is **1:1:1:1:1:1:1:1**.

1.5.6 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. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregateport interface configuration mode.

  interface aggregateport *interface-number*

(4) Configure the minimum guaranteed bandwidth and maximum limited bandwidth for a queue on an interface.

qos queue *queue-id* **bandwidth** { **maximum** *bandwidth* | **minimum** *bandwidth* }

No minimum guaranteed bandwidth or maximum limited bandwidth is configured for a queue by default.

1.6 Configuring the QoS Global Policy

1.6.1 Overview

Enabling the QoS global policy enables some QoS policies by default, for example, changing the DSCP value of L2 flows.

1.6.2 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

The global QoS policy is enabled by default.

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.

Caution

Running the **clear** commands may interrupt services due to loss of important information.

Table 1-2 QoS Monitoring

Command	Purpose
show class-map [*class-map-name*]	Displays the traffic classification information.
show class-map nameid	Displays the mapping between class names and IDs.

Command	Purpose
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 policy-map nameid	Displays the mapping between policy names and IDs.
show virtual-group { *virtual-group-number* | **summary** }	Displays information about a logical interface group.
show mls qos capacity	Displays QoS capabilities.
show mls qos features	Displays chip QoS capabilities.
show mls qos interface { *interface-type interface-number* | **policers** }	Displays the QoS information of an interface.
show mls qos intf_status	Displays the policy application status of all interfaces.
show mls qos istat [**interface** *interface-type interface-number*]	Displays the QoS capabilities and default information on an interface.
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 mstat	Displays the memory usage statistics of QoS.
show mls qos rate-limit [**interface** *interface-type interface-number*]	Displays the rate limit information of an interface.
show mls qos mstat	Displays the memory usage statistics of QoS.
show mls qos virtual-group { *virtual-group-number* | **policers** }	Displays information about a policy applied to a logical interface group.
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.
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.

Command	Purpose
show qos res [**dev** *dev-number* [**slot** *slot-number*]]	Displays QoS resource usage of the current device.
clear qos res	Clears historical peak values of QoS resource usage.
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.

1.8 Configuration Examples

1.8.1 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:

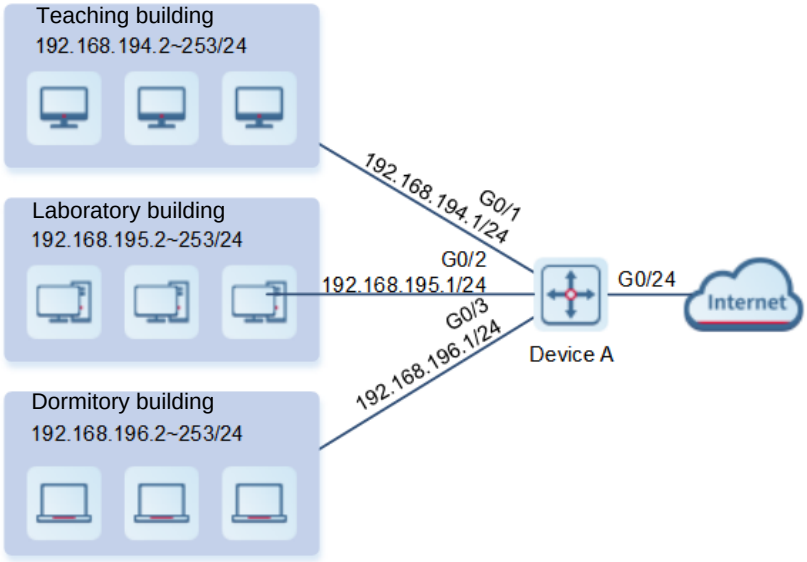
- Controlling the Internet access traffic of the school within 100 Mbps and discarding the packets out of the limit.
- Controlling the egress traffic of the dormitory building within 50 Mbps and discarding the packets out of limit.
- Controlling the rate of packets with DSCP priority 7 sent from laboratory building within 20 Mbps, and discarding the packets out of limit.
- 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 1-6 Topology of Configuring 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 drop
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 drop
```

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 drop
!
interface GigabitEthernet 0/1
 ip address 192.168.194.1 255.255.255.0
 rate-limit input 30720 256
!
interface GigabitEthernet 0/2
 ip address 192.168.195.1 255.255.255.0
 service-policy input pmap_shiyan
 mls qos trust dscp
!
interface GigabitEthernet 0/3
 ip address 192.168.196.1 255.255.255.0
 rate-limit input 51200 256
!
interface GigabitEthernet 0/24
 rate-limit output 102400 256
!
end
```

1.8.2 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.

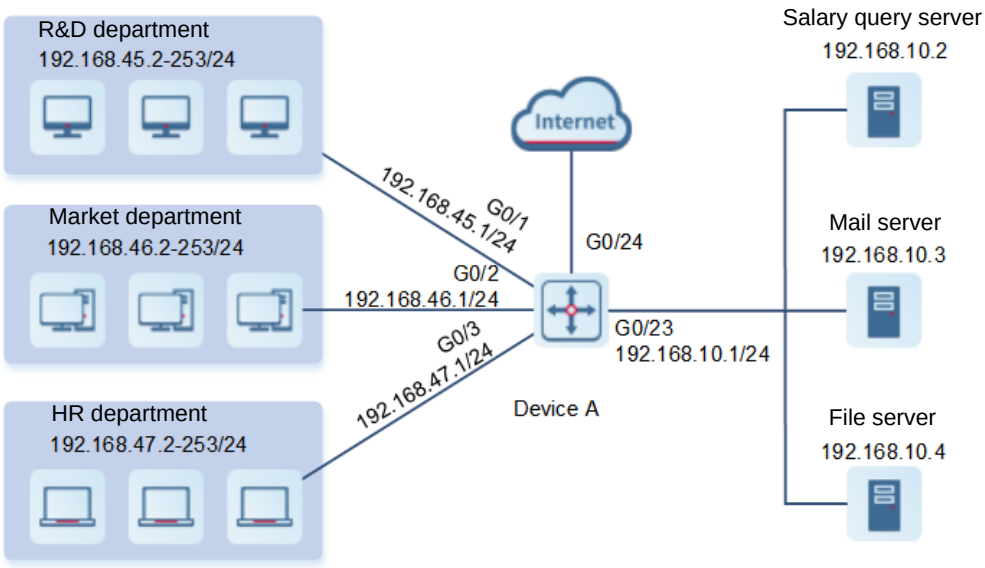
- Network congestion often occurs during operation of device A. WRR queue scheduling must be used to schedule IP packets from the R&D and market departments to access the mail database, file database, and salary query database based on the ratio of 6:2:1.

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 1-7 Topology of Configuring 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) Set the lower thresholds to 10 and 20 for queue 2 of interface G0/2.

(6) Set the higher thresholds to 60 and 90 for queue 2 of interface G0/2.

(7) 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.

Associate a class named salary with the ACL rule 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
```

Associate a class named mail with the ACL rule 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
```

Associate a class named file with the ACL rule 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 the policy named toserver to access the server.

```
DeviceA(config)# policy-map toserver
DeviceA(config-pmap)#
```

Associate the class named salary with a traffic behavior.

```
DeviceA(config-pmap)# class salary
DeviceA(config-pmap-c)# set cos 2
```

```
DeviceA(config-pmap-c)# exit
```

Associate the class named mail with a traffic behavior.

```
DeviceA(config-pmap)# class mail
DeviceA(config-pmap-c)# set cos 4
DeviceA(config-pmap-c)# exit
```

Associate the class named file with a traffic behavior.

```
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 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 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
```

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
!
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 address 192.168.45.1 255.255.255.0
 service-policy input toserver
 mls qos trust cos
!
interface GigabitEthernet 0/2
 ip address 192.168.46.1 255.255.255.0
 service-policy input toserver
 mls qos trust cos
!
interface GigabitEthernet 0/3
 ip address 192.168.47.1 255.255.255.0
 mls qos cos 7
!
```

Security Configuration

1. Configuring AAA
2. Configuring RADIUS
3. Configuring TACACS
4. Configuring IEEE 802.1X
5. Configuring Web Authentication
6. Configuring SCC
7. Configuring Password Policy
8. Configuring SSH
9. Configuring Global IP-MAC Address Binding
10. Configuring Port Security
11. Configuring IP Source Guard
12. Configuring IPv6 Source Guard
13. Configuring SAVI
14. Configuring ARP Check
15. Configuring DAI
16. Configuring ARP Spoofing Prevention
17. Configuring CPP
18. Configuring NFPP
19. Configuring Storm Control
20. Configuring DoS Protection

21. Configuring Security Log Auditing

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 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 8
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 9
1.5.3 Configuration Tasks 9
1.5.4 Configuring Login Authentication 12
1.5.5 Configuring Enable Authentication 13
1.5.6 Configuring IEEE 802.1X Authentication 13
1.5.7 Configuring 2nd-Generation Web Authentication 14
1.5.8 Configuring ClearPass Authentication 16
1.5.9 Configuring FTP Authentication 18
1.6 Configuring a General Authentication Method 19
1.6.1 Overview 19
1.6.2 Restrictions and Guidelines 19

1.6.3 Procedure 19
1.7 Configuring AAA Authentication Logging 19
1.7.1 Overview 19
1.7.2 Procedure 19
1.8 Configuring Basic Features of AAA Authorization 20
1.8.1 Overview 20
1.8.2 Restrictions and Guidelines 20
1.8.3 Procedure 20
1.9 Configuring the Function of Caching Command Authorization Results 21
1.9.1 Overview 21
1.9.2 Restrictions and Guidelines 21
1.9.3 Procedure 21
1.10 Configuring the Default Role for AAA Users 22
1.10.1 Overview 22
1.10.2 Restrictions and Guidelines 22
1.10.3 Procedure 22
1.11 Configuring Basic Features of AAA Accounting 22
1.11.1 Overview 22
1.11.2 Restrictions and Guidelines 22
1.11.3 Procedure 23
1.12 Configuring a Policy for User Accounting Start Failures 24
1.12.1 Overview 24
1.12.2 Procedure 24
1.13 Configuring Domain-Based AAA Services 24

1.13.1 Overview 24
1.13.2 Restrictions and Guidelines 24
1.13.3 Procedure 24
1.14 Enabling the AAA Heartbeat Keepalive Function 25
1.14.1 Overview 25
1.14.2 Restrictions and Guidelines 25
1.14.3 Procedure 26
1.15 Monitoring 26
1.16 Configuration Examples 27
1.16.1 Configuring Local Login Authentication and Local EXEC Authorization 27
1.16.2 Configuring Enable Authentication 29
1.16.3 Configuring Command Authorization 30
1.16.4 Configuring Network Authorization 32
1.16.5 Configuring an AAA Server Group 33
1.16.6 Configuring Domain-based AAA Services 34

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 sections 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.

Caution

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.

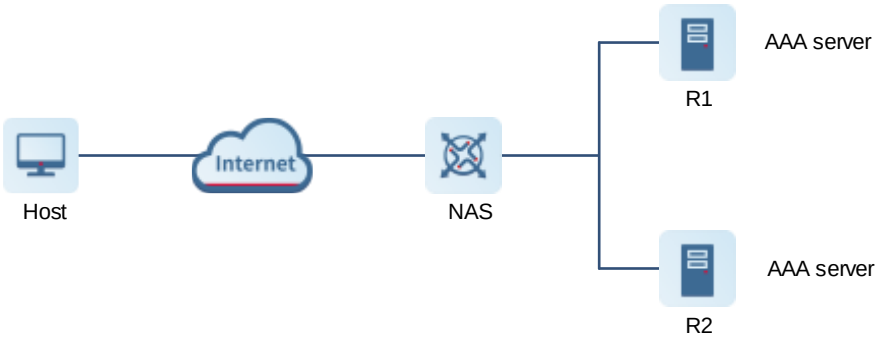
- AAA server group

  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.

Note

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*.

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*.
- Common errors:
  - When the AAA security service is provided using the local method, user information is not configured in the local database.
  - When the AAA security service is provided using the remote server group method, the RADIUS or TACACS+ server is not configured, or user information is not configured in the server.

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*.
- 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 and enter the server group configuration mode.

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.

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
- By default, no username is specified.

  After this command is executed, the device uses **$enab[*level*]$** to send an authentication request to the RADIUS server when you enter the privileged EXEC mode by using the **enable** *level* command. When the entered password matches the password of **$enab[*level*]$** on the RADIUS server, the authentication succeeds.
- Configuring IEEE 802.1X Authentication
- Configuring 2nd-Generation Web Authentication
- Configuring ClearPass Authentication

1. Overview

The ClearPass server can function as the Portal server to connect to the web authentication component, directing authenticated users to the authentication page for authentication.

2. Restrictions and Guidelines

- The device can only connect to the ClearPass server of Aruba that functions as the Portal server for ClearPass authentication.
- When you configure the ClearPass authentication service, you need to configure a ClearPass authentication template, enable the local HTTP server, and configure the IP addresses of the ClearPass server and the NAS device where the authentication service resides as authentication-free resources.

- The ClearPass web authentication server can exchange only HTTP packets with the ClearPass server.
- For details of the web configuration, see "Web Authentication" in *Security Configuration*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the AAA security service.

aaa new-model

The AAA security service is disabled by default.

In ClearPass authentication, the device initiates authentication requests to the server, which is implemented by 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 address, port number, or key is configured for a RADIUS server by default. The default authentication port number is 1812 and the default accounting port number is 1813.

User account information is stored on the RADIUS server. The device needs to connect to the RADIUS server to confirm user identity.

(5) Configure a method list for ClearPass authentication on the device.

aaa authentication cpweb { **default** | *list-name* } { [**group** *group-name*]&<1-4> | **group radius** | **local** | **none** }

No ClearPass authentication method list is configured by default.

The authentication method list associates the web authentication request with the RADIUS server. The device selects an authentication method and the corresponding server based on the authentication method list.

(6) Configure the network accounting method list.

aaa accounting network { **default** | *list-name* } **start-stop** { [**group** *group-name*]&<1-4> | **group radius** | **group tacacs+** | **none** }

The network accounting feature is disabled by default.

The accounting method is used to associate the accounting method with a server. Web authentication needs the accounting feature to record user information or fees.

(7) Create a ClearPass authentication template and enter the ClearPass authentication template configuration mode.

web-auth template cpweb

(8) Configure web authentication template parameters.

a Configure an IP address and a VRF instance for the Portal server.

ip [*ipv4-address*]

No IP address is configured for the Portal server by default.

b Configure a page address for the Portal server.

url *url-string*

A page address is configured for the Portal server by default.

c Configure the URL format for redirection packets.

fmt { custom | clearpass }

The URL of the redirection packets use the ClearPass URL format by default.

d Configure a method used by the device to parse authentication requests.

http-method post [username-key usrkey-string] *[* password-key pswkey-string] [init-url-key urlkey-string] [**password-encrypt** { **none** | **uam** }]

The identified username is **username** and the password is **password** not encrypted, by default.

e Configure the redirection packet format.

redirect { **http** | **js** }

Redirection packets are in JS format by default.

f Configure a response method after successful authentication.

login-success response { redirect-init-url [*default-url* def-string] | msg msg-string | redirect-url *url-string* }

The device pops the default page after successful authentication by default.

g Configure a response method after authentication failure.

login-fail response { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] | **msg** *msg-string* }

The device redirects to the authentication page after an authentication failure by default.

h Configure whether to pop the active logoff page after successful authentication. (This command takes effect only after a redirection URL for successful authentication is configured.)

logout-popup-window

This feature is disabled by default.

(9) Configure a communication IP address for the HTTP server.

web-auth auth-server ip { *ipv4-address* }

No communication IP address is configured for the HTTP server by default.

(10) Configure a communication port for the HTTP server.

web-auth auth-server http [*port*]

No communication port is configured for the HTTP server by default.

(11) Configure the URL used by the terminal to initiate authentication.

web-auth auth-server submit-url {*url-string*}

The URL used by the terminal to initiate authentication is not configured by default.

(12) Exit to the global configuration mode.

exit

(13) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

(14) Enable ClearPass authentication on the interface.

web-auth enable cpweb

ClearPass authentication is disabled on the interface by default.

- 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.

(5) (Optional) Configure **$enab[*level*]$** as the username when you configure Enable authentication through the RADIUS server. The value range of *level* is from 0 to 15.

aaa authentication enable private-user

By default, no username is specified.

After this command is executed, the device uses **$enab[*level*]$** to send an authentication request to the RADIUS server when you enter the privileged EXEC mode by using the **enable** *level* command. When the entered password matches the password of **$enab[*level*]$** on the RADIUS server, the authentication succeeds.

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*.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *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

- For details about Web authentication configuration, see *Configuring Web Authentication*.

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* | **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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *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 ClearPass Authentication

1. Overview

The ClearPass server can function as the Portal server to connect to the web authentication component, directing authenticated users to the authentication page for authentication.

2. Restrictions and Guidelines

- The device can only connect to the ClearPass server of Aruba that functions as the Portal server for ClearPass authentication.
- When you configure the ClearPass authentication service, you need to configure a ClearPass authentication template, enable the local HTTP server, and configure the IP addresses of the ClearPass server and the NAS device where the authentication service resides as authentication-free resources.
- The ClearPass web authentication server can exchange only HTTP packets with the ClearPass server.
- For details of the web configuration, see "Web Authentication" in *Security Configuration*.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the AAA security service.

aaa new-model

The AAA security service is disabled by default.

In ClearPass authentication, the device initiates authentication requests to the server, which is implemented by 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 address, port number, or key is configured for a RADIUS server by default. The default authentication port number is 1812 and the default accounting port number is 1813.

User account information is stored on the RADIUS server. The device needs to connect to the RADIUS server to confirm user identity.

(5) Configure a method list for ClearPass authentication on the device.

aaa authentication cpweb { **default** | *list-name* } { [**group** *group-name*]&<1-4> | **group radius** | **local** | **none** }

No ClearPass authentication method list is configured by default.

The authentication method list associates the web authentication request with the RADIUS server. The device selects an authentication method and the corresponding server based on the authentication method list.

(6) Configure the network accounting method list.

aaa accounting network { **default** | *list-name* } **start-stop** { [**group** *group-name*]&<1-4> | **group radius** | **group tacacs+** | **none** }

The network accounting feature is disabled by default.

The accounting method is used to associate the accounting method with a server. Web authentication needs the accounting feature to record user information or fees.

(7) Create a ClearPass authentication template and enter the ClearPass authentication template configuration mode.

web-auth template cpweb

(8) Configure web authentication template parameters.

a Configure an IP address and a VRF instance for the Portal server.

ip [*ipv4-address*]

No IP address is configured for the Portal server by default.

b Configure a page address for the Portal server.

url *url-string*

A page address is configured for the Portal server by default.

c Configure the URL format for redirection packets.

fmt { custom | clearpass }

The URL of the redirection packets use the ClearPass URL format by default.

d Configure a method used by the device to parse authentication requests.

http-method post [**username-key** *usrkey-string*] [**password-key** *pswkey-string*] [**init-url-key** *urlkey-string*] [**password-encrypt** { **none** | **uam** }]

The identified username is **username** and the password is **password** not encrypted, by default.

e Configure the redirection packet format.

redirect { **http** | **js** }

Redirection packets are in JS format by default.

f Configure a response method after successful authentication.

login-success response { **redirect-init-url** [**default-url** *def-strin*g] | **msg** *msg-string* | **redirect-url** *url-string* }

The device pops the default page after successful authentication by default.

g Configure a response method after authentication failure.

login-fail response { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] | **msg** *msg-string* }

The device redirects to the authentication page after an authentication failure by default.

h Configure whether to pop the active logoff page after successful authentication. (This command takes effect only after a redirection URL for successful authentication is configured.)

logout-popup-window

This feature is disabled by default.

(9) Configure a communication IP address for the HTTP server.

web-auth auth-server ip { *ipv4-address* }

No communication IP address is configured for the HTTP server by default.

(10) Configure a communication port for the HTTP server.

web-auth auth-server http [*port*]

No communication port is configured for the HTTP server by default.

(11) Configure the URL used by the terminal to initiate authentication.

web-auth auth-server submit-url {*url-string*}

The URL used by the terminal to initiate authentication is not configured by default.

(12) Exit to the global configuration mode.

exit

(13) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

(14) Enable ClearPass authentication on the interface.

web-auth enable cpweb

ClearPass authentication is disabled on the interface by default.

1.5.9 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*.

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 command authorization method list to authorize permitted users to run a command.

  aaa authorization commands *level* { **default** | *list-name* } *method*&<1-4>

No command 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*.

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.
- After domain name-based AAA service is enabled, you can run the **aaa domain disable** command to switch the domain name-based service to global service for 802.1x, Enable, Login, and Web authentication users separately.

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 AAA 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** | **web-auth** } { **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.

(11) (Optional) Disable the domain name-based AAA service for the specified authentication user.

aaa domain disable { **dot1x** | **enable** | **login** | **web-auth** }

By default, the domain name-based AAA service is not disabled for 802.1x and Web authentication users. Campus products do not configure the domain name-based AAA service for Enable and Login authentication users. DCN products configure the domain name-based AAA service for Enable and Login authentication users.

1.14 Enabling the AAA Heartbeat Keepalive Function

1.14.1 Overview

The heartbeat keepalive function in the AAA module is used to solve the problem that the AAA function is unavailable due to abnormal internal disconnection under special circumstances.

1.14.2 Restrictions and Guidelines

The interval for sending heartbeat messages is 60s, which has little impact on performance; therefore, it is recommended to enable this function.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the AAA heartbeat keepalive function.

aaa heartbeat enable

By default, the AAA heartbeat keepalive function is enabled.

1.15 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 AAA Monitoring

Command	Purpose
show aaa accounting update	Displays accounting update information.
show aaa capability	Displays AAA-related capabilities.
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.

1.16 Configuration Examples

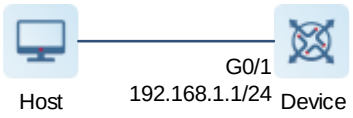
1.16.1 Configuring Local Login Authentication and Local EXEC Authorization

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 Abc123456
Device(config)# username host2 privilege 4 password Abc12345
```

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: Abc123456



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: Abc12345



Device# show privilege
Current privilege level is 4
```

6. Configuration Files

```
!
username host1 privilege 15 password 7 $10$3b0$VyesigqNRs04$
username host2 privilege 4 password 7 $10$05f$wL8+5zw6/EY=$
!
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.

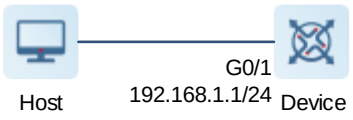
1.16.2 Configuring Enable Authentication

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.

Note

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 Abc123456
```

Set the password to **Abc123456** for privilege level 15 in Enable authentication.

```
Device(config)# enable secret level 15 Abc123456
```

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: Abc123456



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** (**Abc123456**) for authentication to successfully switch the privilege level to 15.

```
Device# enable 15
Password: Abc123456

Device# show privilege
Current privilege level is 15
```

6. Configuration Files

```
!
username host1 privilege 15 password 7 $10$3b0$VyesigqNRs04$
!
aaa new-model
!
aaa authentication enable default local enable
!
enable secret 8 $1c$js8h23u42A$:$6v$ln48$,|0.pl!:rtbr$:#h.j.462j$n,f.`($
!
end
```

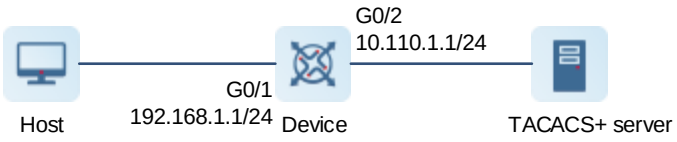
1.16.3 Configuring Command Authorization

1. Requirements

Command authorization needs to be configured for login users so that users who log in to the device through terminals can only use commands in their authorized scopes.

2. Topology

Figure 1-4 Topology of Command Authorization



3. Notes

- Enable AAA security services on the device.
- Configure an IP address and a shared key for the TACACS+ server on the device.
- Configure the login authentication method list and command authorization method list on the device.
- Configure to-be-authenticated users and authorized command scopes on the TACACS+ server.
- Apply the authentication method and authorization method to a specific line.

4. Procedure

(1) On the TACACS+ server, add login users, configure authorized command scopes, and configure the server to provide AAA services for the device. (The configuration is omitted here. For the configuration of the TACACS+ server, use the operation manual of the server.)

(2) Enable AAA security services.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

(3) Configure the IP address and shared key of the TACACS+ server (the IP address is set to **10.110.1.2** and shared key to **sharekey** in this example).

```
Device(config)# tacacs-server host 10.110.1.2 key sharekey
```

(4) Configure a login authentication method list named **login-method**, in which TACACS+ server authentication is prior to local authentication.

```
Device(config)# aaa authentication login login-method group tacacs+ local
```

(5) Add the account **host1** to the local user database and configure the account permissions.

```
Device(config)# username host1 privilege 15 password Abc123456
```

(6) Configure a command authorization method list named **command-method** for level-15 commands. In this list, TACACS+ server authorization is prior to local authorization.

```
Device(config)# aaa authorization commands 15 command-method group tacacs+ local
```

(7) 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 command-method
```

5. Common Errors

- The shared key configured on the TACACS+ server is different from that configured on the device.

- A command authorization configuration error occurs on the TACACS+ server.

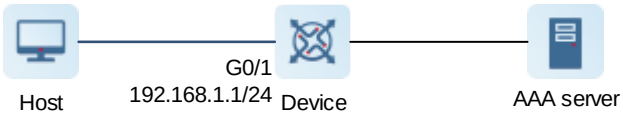
1.16.4 Configuring Network Authorization

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 1-5 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
!
```

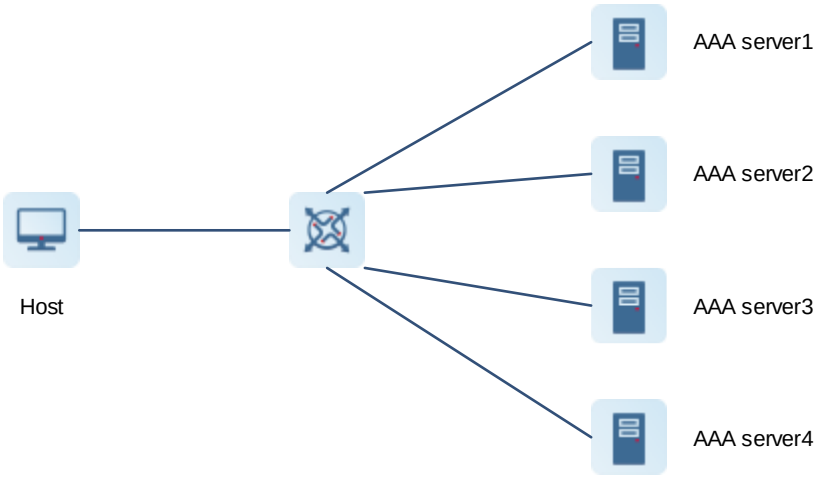
1.16.5 Configuring an AAA Server Group

1. Requirements

A custom AAA server group needs to be created to provide AAA services.

2. Topology

Figure 1-6 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.

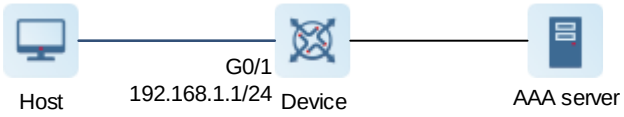
1.16.6 Configuring Domain-based AAA Services

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 1-7 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
!
```

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 Enabling Dynamic Extension Authorization on the RADIUS Server 10

1.4.1 Overview 10

1.4.2 Restrictions and Guidelines 10

1.4.3 Procedure 10

1.5 Configuring a RADIUS Server Group 11

1.5.1 Overview 11

1.5.2 Restrictions and Guidelines 11

1.5.3 Procedure 11

1.6 Configuring RADIUS Attributes 12

1.6.1 Overview 12

1.6.2 Configuration Tasks 12

1.6.3 Configure the Attribute Format 12

1.6.4 Configuring Ruijie Private Attributes 13

1.6.5 Configuring Compatibility with Devices of Other Vendors 14
1.7 Configuring RADIUS Reachability Detection 15
1.7.1 Overview 15
1.7.2 Restrictions and Guidelines 15
1.7.3 Procedure 15
1.8 Configuring the Units of Data Flows and Packets to Be Sent to a RADIUS Server 16
1.8.1 Overview 16
1.8.2 Procedure 16
1.9 Configuring the Accounting-On Function 17
1.9.1 Overview 17
1.9.2 Procedure 17
1.10 Configuring the Accounting Packet Copying Function 17
1.10.1 Overview 17
1.10.2 Procedure 17
1.11 Monitoring 18
1.12 Configuration Examples 19
1.12.1 Configuring RADIUS Authentication, Authorization, and Accounting 19
1.12.2 Configuring RADIUS Reachability Detection 20

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.

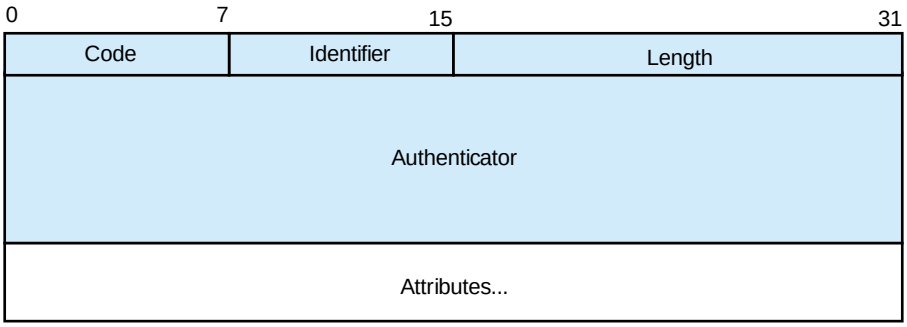
  If multiple RADIUS servers are configured in a RADIUS server group, when a device fails to communicate with the first RADIUS server or the first RADIUS server is unreachable, the device automatically attempts

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

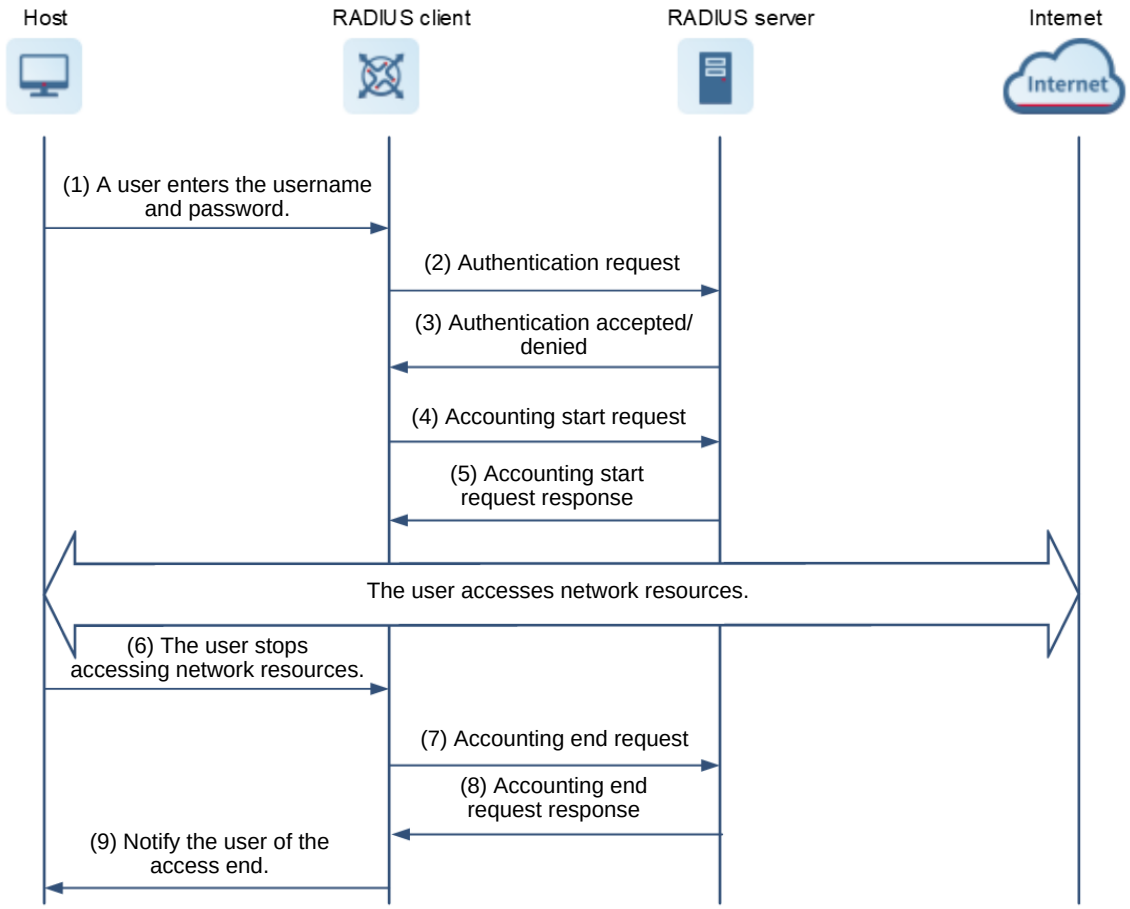
ID	Function	Type	Extended Type
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	VLAN-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	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.

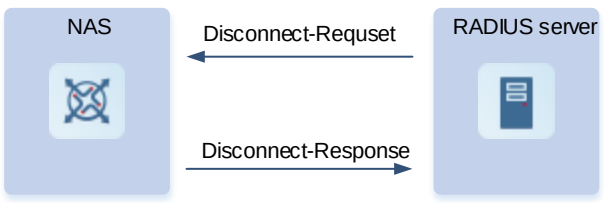
- Retransmission count
- Whether accounting update packets need to be retransmitted

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

- RFC 2865: Remote Authentication Dial In User Service (RADIUS)
- RFC 2866: RADIUS Accounting
- RFC 2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868: RADIUS Attributes for Tunnel Protocol Support
- RFC 2869: RADIUS Extensions
- RFC 3576: 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) (Optional)Enabling Dynamic Extension Authorization on the RADIUS Server

(3) Configuring a RADIUS Server Group

(4) (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

(5) (Optional) Configuring RADIUS Reachability Detection

(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 { *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.

(9) (Optional) Enable the compatibility of encapsulated user name.

radius user-name compatible

By default, the compatibility of encapsulated user name is disabled.

After this function is enabled, the user names in RADIUS packets are encapsulated in the customer-specific format, rather than the UTF-8 format.

(10) (Optional) Configure the value of the NAS-IP-Address field in RADIUS packets.

radius-server nas-ip-address key { *ipv4-address* | *ipv6-address* }

By default, the value of the NAS-IP-Address field is not configured.

(11) (Optional) Configure the NAS-ID field in RADIUS packets.

radius-server nasid *nas-id*

The NAS-ID field in RADIUS packets is not configured by default.

1.4 Enabling Dynamic Extension Authorization on the RADIUS Server

1.4.1 Overview

After dynamic extension authorization of the RADIUS server is configured, the device can process dynamic extension authorization packets (such as DM or COA packets), allowing the server to perform dynamic authorization operations such as disconnecting online users and ACL authorization.

1.4.2 Restrictions and Guidelines

- The server can perform dynamic authorization for online users only when the server supports dynamic extension authorization and the device is enabled with dynamic extension authorization.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable dynamic extension authorization on the RADIUS server.

radius dynamic-authorization-extension enable

Dynamic extension authorization on the RADIUS server is enabled by default.

(4) Configure the communication port for dynamic extension authorization packets of the RADIUS server.

radius dynamic-authorization-extension port port-number

The default communication port for dynamic extension authorization packets of the RADIUS server is 3799.

(5) (Optional)Enable dynamic extension authorization of the RADIUS server to check the RADIUS timestamp.

radius dynamic-authorization-extension attribute check event-timestamp

The device is not enabled with dynamic extension authorization of the RADIUS server to check the RADIUS timestamp by default.

(6) (Optional) Enable dynamic extension authorization of the RADIUS server to check duplicate packets.

radius dynamic-authorization-extension duplicate-packet discard

The device is not enabled with dynamic extension authorization of the RADIUS server to check duplicate packets by default.

(7) (Optional) Enable the RADIUS server to check the timestamp in dynamic extension authorization packets.

radius dynamic-authorization-extension event-timestamp interval *interval-value*

The RADIUS server is not enabled to check the timestamp in dynamic extension authorization packets by default.

(8) (Optional) Configure the maximum number of dynamic extension authorization packets of the RADIUS server that the device can process concurrently.

radius dynamic-authorization-extension max-req *max-req-value*

The maximum number of dynamic extension authorization packets of the RADIUS server that the device can process concurrently is not configured by default.

(9) (Optional) Configure the timeout interval of dynamic extension authorization response packets of the RADIUS server.

radius dynamic-authorization-extension timeout *timeout-value*

The default timeout interval of dynamic extension authorization response packets of the RADIUS server is 30 seconds.

1.5 Configuring a RADIUS Server Group

1.5.1 Overview

One or more RADIUS servers can be added to each RADIUS server group, which provides AAA services for users as a whole.

1.5.2 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**.

1.5.3 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.

1.6 Configuring RADIUS Attributes

1.6.1 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.

1.6.2 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

1.6.3 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.

1.6.4 Configuring Ruijie Private Attributes

1. Overview

Vendors can define private attributes to implement multiple 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.

1.6.5 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.

1.7 Configuring RADIUS Reachability Detection

1.7.1 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.

1.7.2 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.

1.7.3 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*

The default duration for the device to stop sending request messages to an unreachable RADIUS security server is 5 minutes.

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.

1.8 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) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) 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** command to check the configuration.

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

Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 1-6 RADIUS Monitoring

Command	Purpose
show radius acct statistics	Displays RADIUS accounting statistics.
show radius attribute	Displays RADIUS standard attributes.
show radius auth statistics	Displays RADIUS authentication statistics.
show radius dynamic-authorization-extension statistics	Displays information about dynamic extension authorization packets.
show radius group	Displays the configuration of a RADIUS server group.
show radius parameter	Displays global parameters of a RADIUS server.
show radius server	Displays the configuration of a RADIUS server.
show radius timeout record	Displays timeout of outgoing RADIUS packets.
show radius vendor-specific	Displays the configuration of the RADIUS private attribute type.
show radius-server accounting-copy [**interface** *interface-type interface-number*]	Displays the configuration of copying RADIUS accounting packets and sending them to servers in a specified server group.
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

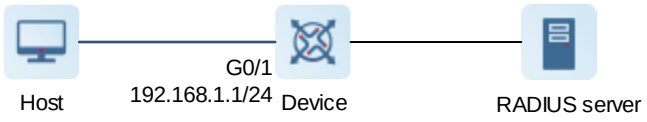
1.12.1 Configuring RADIUS Authentication, Authorization, and Accounting

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.

(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:Abc123456



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.

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.

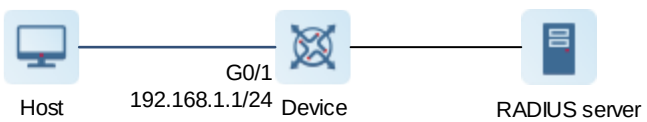
1.12.2 Configuring RADIUS Reachability Detection

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# 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+.

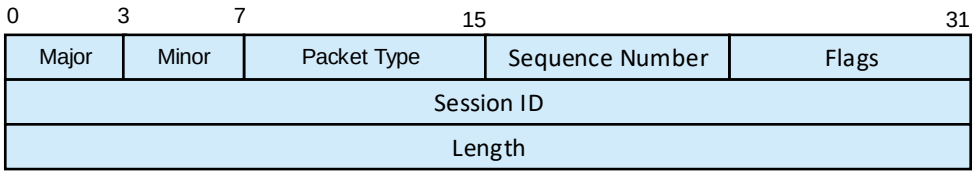
Both TACACS+ and Remote Authentication Dial-In User Service (RADIUS) are capable of providing AAA security services. Compared with RADIUS, TACACS+ has the following advantages:

- 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.

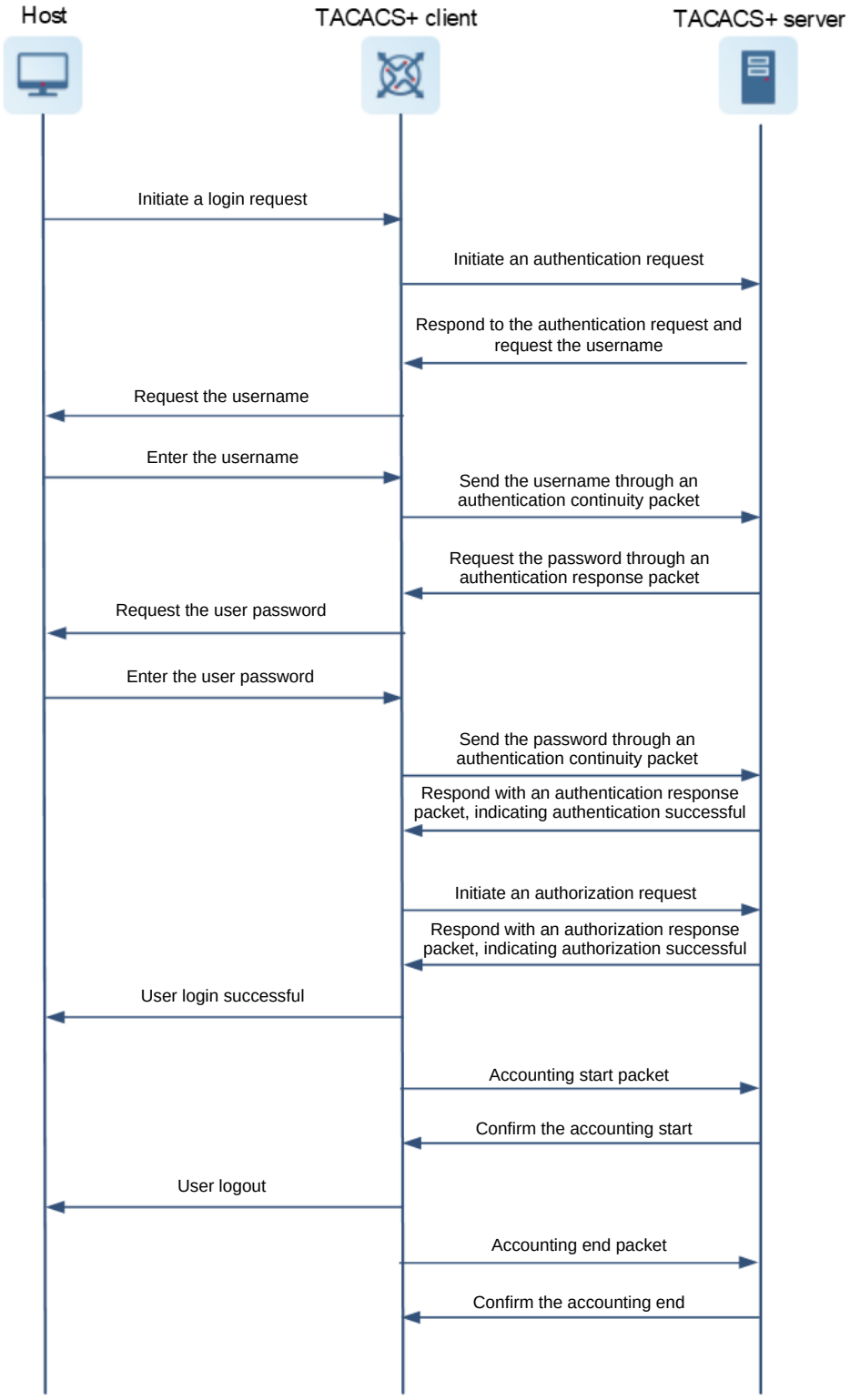
Table 1-1 Description of Fields Contained in a TACACS+ Packet

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 { *ipv4-address* | *ipv6-address* } [**port** *port-number* | **single-connection** | **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.

(8) (Optional) Configure the maximum keepalive time of TCP sessions in single-connection mode.

tacacs-server single-connect-timeout *single-connect-timeout*

By default, the maximum keepalive time of TCP sessions in single-connection mode is 30 minutes.

When the device communicates with a TACACS server in single-connection mode, the device actively tears down the connection if the TCP session exceeds the maximum keepalive time. If the device needs to communicate with the TACACS server again, it should set up the TCP session again.

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* } [**single-connection**]

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) (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 configuration.

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 1-2 TACACS+ Monitoring

Command	Purpose
show tacacs	Displays the interaction between the device and each TACACS+ server.
show tacacs server	Displays statistics on a TACACS+ server group.
debug tacacs+	Debugs TACACS+.

1.7 Configuration Examples

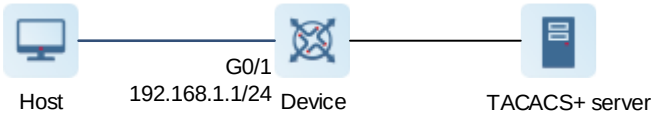
1.7.1 Configuring TACACS+ for Login Authentication

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.

(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: Abc123456



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.

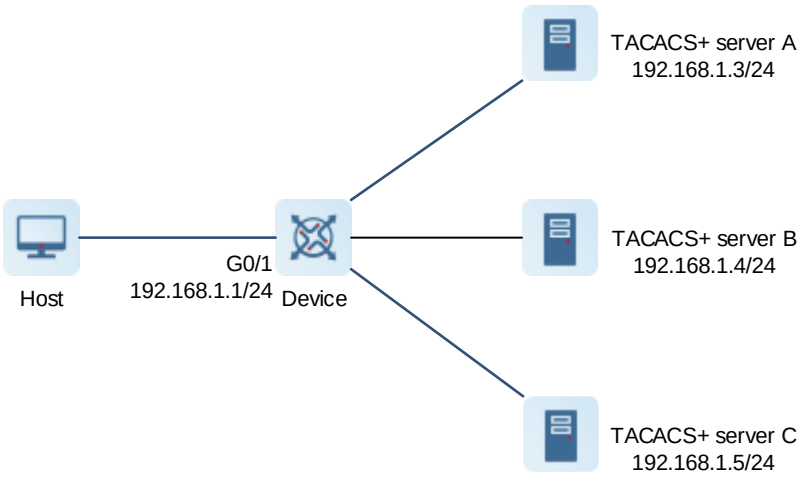
1.7.2 Configuring Separated Authentication, Authorization and Accounting by Using TACACS+

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.

(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 tacacs-method
Device(config-line)# authorization exec radius-method
Device(config-line)# accounting exec radius-method
```

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: Abc123456



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.

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.

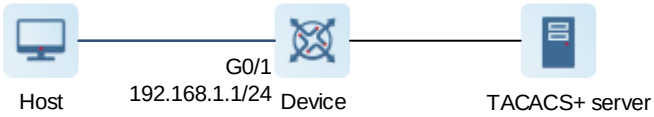
1.7.3 Configuring Reachability Detection

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# 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:
   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 9

1.3.1 Overview 9

1.3.2 Restrictions and Guidelines 9

1.3.3 Prerequisites 10

1.3.4 Procedure 10

1.4 Configuring IEEE 802.1X Parameters 11

1.4.1 Overview 11

1.4.2 Configuration Tasks 11

1.4.3 Configuring Re-authentication 12

1.4.4 Configuring Packet Retransmission Parameters 12

1.4.5 Configuring the Server Timeout Duration 13

1.4.6 Configuring the Quiet Period After an Authentication Failure 13

1.4.7 Configuring the Authentication Mode 14

1.4.8 Configuring Ruijie Client Detection 14

1.4.9 Configuring Automatic Domain Name Supplement for 802.1X Users 15

1.5 Configuring Authorization 16

1.5.1 Overview 16

1.5.2 Restrictions and Guidelines 16
1.5.3 Procedure 16
1.6 Configuring MAB 17
1.6.1 Overview 17
1.6.2 Restrictions and Guidelines 17
1.6.3 Configuration Tasks 17
1.6.4 Configuring Single-User MAB 18
1.6.5 Configuring Multi-User MAB 18
1.7 Configuring MAB Parameters 20
1.7.1 Overview 20
1.7.2 Configuration Tasks 20
1.7.3 Configuring the Username Format for MAB 21
1.7.4 Configuring the Username Uppercase/Lowercase for MAB 21
1.7.5 Enabling Domain Name Completion for MAB Users 22
1.7.6 Configuring MAB VLAN 23
1.7.7 Configuring the MAB Timeout Duration 23
1.7.8 Enabling Fast MAB 23
1.7.9 Configuring a Permanent License 24
1.8 Configuring IAB 24
1.8.1 Overview 24
1.8.2 Restrictions and Guidelines 24
1.8.3 Procedure 25
1.9 Configuring the Port Control Mode 26
1.9.1 Overview 26

1.9.2 Configuration Tasks 26
1.9.3 Configuring the MAC-based Control Mode 26
1.9.4 Configuring the Port-based Control Mode 26
1.10 Configuring Automatic Dynamic VLAN Redirection on IEEE 802.1X Ports 28
1.10.1 Overview 28
1.10.2 Restrictions and Guidelines 28
1.10.3 Procedure 29
1.11 Configuring the Guest VLAN Function 30
1.11.1 Overview 30
1.11.2 Restrictions and Guidelines 30
1.11.3 Procedure 30
1.12 Configuring the Failed VLAN Function 31
1.12.1 Overview 31
1.12.2 Restrictions and Guidelines 31
1.12.3 Procedure 31
1.13 Configuring Extended Features 32
1.13.1 Overview 32
1.13.2 Configuration Tasks 32
1.13.3 Enabling Active Authentication 33
1.13.4 Configuring a List of Hosts Allowed for Authentication 34
1.13.5 Disabling the Virtual Source MAC Address Function 34
1.13.6 Configuring Multi-Account Authentication with One MAC Address 35
1.13.7 Configuring the Maximum Number of Users Who Can Be Authenticated on an Interface 35
1.13.8 Configuring the Function of Initiating Accounting After an IP Address Is Obtained 35

1.13.9 Configuring the Priority Order of IEEE 802.1X and MAB 36
1.13.10 Configuring the Accounting Update Period 36
1.13.11 Configuring Compatibility with H3C Clients and Servers 37
1.13.12 Disabling the Global IEEE 802.1X Features 37
1.13.13 Enabling Perception-free Migration Across VLANs for 802.1X Users 38
1.13.14 Configuring the Function of Instantly Sending Accounting Update Packets Upon IP Address Changes of 802.1X Authenticated Users 38
1.13.15 Converting User Names into TEXT Format 39
1.13.16 Compatible with Third-Party Clients 39
1.13.17 Configuring the Function of Carrying Static IP Addresses in Authentication and Accounting Packets for IEEE 802.1X and MAB 39
1.13.18 Recording Debugging Information to a File 40
1.14 Monitoring 40
1.15 Configuration Examples 42
1.15.1 Configuring IEEE 802.1X Authentication 42
1.15.2 Configuring the IP Authorization Mode 44
1.15.3 Configuring Multi-user MAB 45
1.15.4 Configuring IAB 47
1.15.5 Configuring Automatic Dynamic VLAN Redirection 48
1.15.6 Configuring Guest VLAN 49
1.15.7 Configuring Failed VLAN 51

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

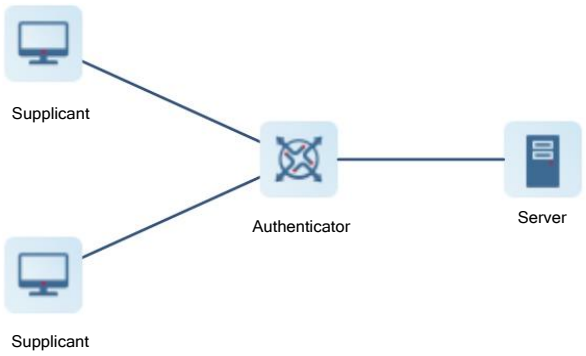
Authentication is a process of verifying user identities and determining whether a user has the legitimate permission to access network resources.

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 is usually a switch.

  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

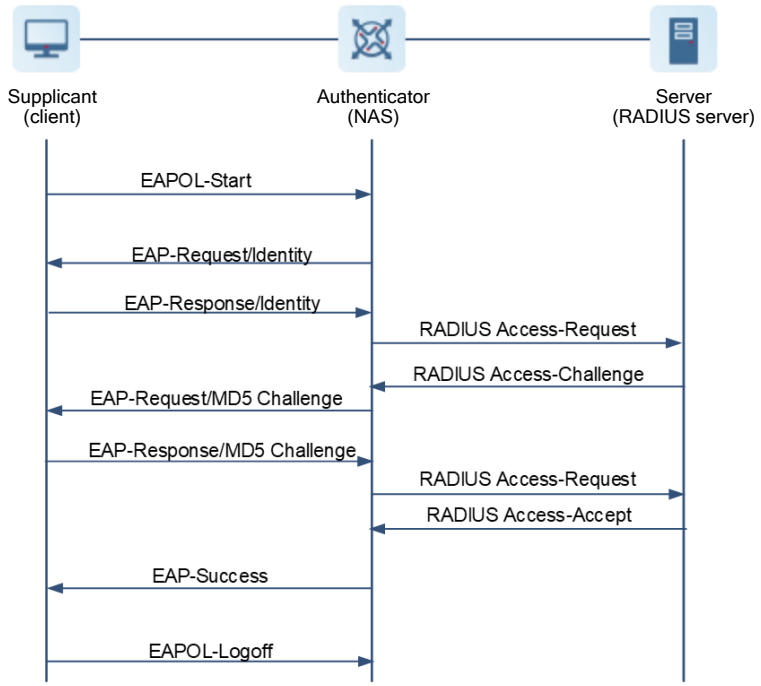


Figure 1-2 shows a typical user-initiated authentication process.

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 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.

- 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 configuration.

- 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.

Caution

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

- IEEE 802.1X: Port-Based Network Access Control
- RFC 2869: 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
- Configuring Automatic Domain Name Supplement for 802.1X Users

(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
- Enabling Domain Name Completion for MAB Users
- Configuring MAB VLAN
- Configuring the MAB Timeout Duration
- Enabling Fast MAB
- Configuring a Permanent License

(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
- Enabling Perception-free Migration Across VLANs for 802.1X Users
- Configuring the Function of Instantly Sending Accounting Update Packets Upon IP Address Changes of 802.1X Authenticated Users
- Converting User Names into TEXT Format
- Compatible with Third-Party Clients
- Configuring the Function of Carrying Static IP Addresses in Authentication and Accounting Packets for IEEE 802.1X and MAB

2. Overview

After this function is configured, when the device receives an ARP packet sent by a terminal with a static IP address, the device reports the static IP address carried in the IEEE 802.1X and MAB authentication and accounting packets.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of carrying static IP addresses in IEEE 802.1X and MAB authentication and accounting packets.

dot1x get-static-ip enable

By default, IEEE 802.1X and MAB authentication do not carry static IP addresses in authentication and accounting packets.

- Recording Debugging Information to a File

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*.
- 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*.
- 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 configuration.

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 { *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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the batch Layer 2 Ethernet interface configuration mode.

  interface range *ethernet-type interface-number*

- Enter the batch Layer 2 link aggregation configuration mode.

  interface range aggregateport *interface-number*

(8) (Optional) Apply 802.1x authentication method list and accounting method list on interface. If the commands are not run on interfaces, the global configuration takes effect.

- Apply 802.1x authentication method list on an interface.

  dot1x authentication { **default** | *list-name* }

- Apply 802.1x accounting method list on an interface.

  dot1x accounting { **default |** *list-name* }

(9) 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
- Configuring Automatic Domain Name Supplement for 802.1X Users

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 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. Restrictions and Guidelines

When local authentication is enabled for 802.1x users, only chap and pap modes are supported.

3. 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.

1.4.9 Configuring Automatic Domain Name Supplement for 802.1X Users

1. Overview

This function is used to automatically supplement the domain name for 802.1X users.

In some domain-based authentication scenarios (AD domain environment of Microsoft), usernames used for authentication must carry the corresponding domain name. The device supports configuration of a domain name for an 802.1X user. The username used by the device to initiate authentication to the authentication server carries the domain name automatically, to meet the environmental requirement of domain-based authentication.

2. Restrictions and Guidelines

- This function can take effect in interface and global configuration modes. The interface configuration prevails.
- This function can detect only string-type domain names suffixed with the at sign (@) and support only automatic domain name supplement using this sign. If the username of a user under authentication contains the at sign (@) and the specified domain name after the at sign (@), it is considered that the username carries a valid domain name and can be directly used for authentication. If the specified domain name is not contained in the username, it is considered that the username does not carry a valid domain name. In this case, the at sign (@) and specified domain name are forcibly added after the username for authentication.

3. Procedure (Global Configuration)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable automatic domain name supplement for 802.1X users in global configuration mode, and specify the domain name that must be carried in the usernames.

dot1x domain-name *name*

Automatic domain name supplement for 802.1X users is globally disabled by default.

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.

interface *interface-type interface-number*

(4) Enable automatic domain name supplement for 802.1X users on an interface, and specify the domain name that must be carried in the usernames.

dot1x domain-name *name*

Automatic domain name supplement for 802.1X users is disabled on an interface by default.

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*.
- 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*.

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.
- When 802.1X users perform authentication for go-online or receive EAP packets on an interface, the interface automatically exits single-user MAB. After the interface changes from the Down state to the Up state or the IEEE802.1X function is enabled, single-user MAB is restored and takes effect again. The interface must meet the preceding conditions to enter the MAB mode. For more information, see Restrictions and Guidelines

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 Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the batch Layer 2 Ethernet interface configuration mode.

(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.
- With the LLDP function, the device can discover phones connected to its ports. If phone MAB is disabled, all devices on the ports access network resources over the Native VLAN after being authenticated. When phone MAB is enabled, the phones access network resources over the Voice VLAN after being authenticated, while non-phone devices still access network resources over the Native VLAN. This improves the call quality of the phones. Phone MAB can be used only when multi-user MAB is supported. If the Voice VLAN is different from the Native VLAN, the phones can access network resources by using the MAC VLAN and VLAN redirection method.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) **(Optional) Enable phone MAB.**

dot1x mult-mab voice-vlan-auth enable

Phone MAB is disabled by default.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the batch Layer 2 Ethernet interface configuration mode.

(5) Enable multi-user MAB.

dot1x mac-auth-bypass multi-user

Multi-user MAB is disabled by default.

(6) (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.

(7) (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**.

(8) (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.

(9) (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
- Enabling Domain Name Completion for MAB Users

1. Overview

This function automatically completes domain names for MAB authentication users.

In some domain-based authentication scenarios (such as Microsoft AD scenario), the authentication user names must carry domain names. The device can configure domain names for MAB authentication users. When the device initiates an authentication request to the authentication server, the sent user name carries a domain name, which meets the domain authentication requirements.

2. Restrictions and Guidelines

This function can be enabled on interfaces or globally. The configuration on interface is prior to the global configuration.

3. Procedure (Global)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global domain name completion function for MAB users and specify the domain name to be carried by MAB users.

dot1x mac-auth-bypass domain-name *name*

By default, the domain name completion function for MAB users is disabled globally.

4. Procedure (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) Enable the domain name completion function for MAB users on the interface and specify the domain name to be carried by MAB users.

dot1x mac-auth-bypass domain-name *name*

By default, the domain name completion function for MAB users is disabled on interfaces.

- Configuring MAB VLAN
- Configuring the MAB Timeout Duration
- Enabling Fast MAB
- Configuring a Permanent License

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 Enabling Domain Name Completion for MAB Users

1. Overview

This function automatically completes domain names for MAB authentication users.

In some domain-based authentication scenarios (such as Microsoft AD scenario), the authentication user names must carry domain names. The device can configure domain names for MAB authentication users. When the device initiates an authentication request to the authentication server, the sent user name carries a domain name, which meets the domain authentication requirements.

2. Restrictions and Guidelines

This function can be enabled on interfaces or globally. The configuration on interface is prior to the global configuration.

3. Procedure (Global)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the global domain name completion function for MAB users and specify the domain name to be carried by MAB users.

dot1x mac-auth-bypass domain-name *name*

By default, the domain name completion function for MAB users is disabled globally.

4. Procedure (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) Enable the domain name completion function for MAB users on the interface and specify the domain name to be carried by MAB users.

dot1x mac-auth-bypass domain-name *name*

By default, the domain name completion function for MAB users is disabled on interfaces.

1.7.6 Configuring MAB VLAN

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the batch Layer 2 Ethernet interface configuration mode.

(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.

1.7.7 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the batch Layer 2 Ethernet interface configuration mode.

(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.

1.7.8 Enabling Fast MAB

1. Overview

After the fast MAB function is enabled, the device can quickly receive MAC addresses and implement MAB in microseconds.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the fast MAB function.

dot1x mac-auth-bypass fast

The fast MAB function is disabled by default.

1.7.9 Configuring a Permanent License

1. Overview

You can configure a permanent license for MAB users.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a permanent license for MAB users.

dot1x mab session-timeout unlimited

The permanent license function is disabled for MAB users by default.

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*. 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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) (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.

(4) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(5) Configure the port-based control mode.

dot1x port-control-mode port-based

A port is controlled based on MAC addresses by default.

(6) (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.

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*). 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 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
- Enabling Perception-free Migration Across VLANs for 802.1X Users
- Configuring the Function of Instantly Sending Accounting Update Packets Upon IP Address Changes of 802.1X Authenticated Users
- Compatible with Third-Party Clients
- Configuring the Function of Carrying Static IP Addresses in Authentication and Accounting Packets for IEEE 802.1X and MAB

1. Overview

After this function is configured, when the device receives an ARP packet sent by a terminal with a static IP address, the device reports the static IP address carried in the IEEE 802.1X and MAB authentication and accounting packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of carrying static IP addresses in IEEE 802.1X and MAB authentication and accounting packets.

dot1x get-static-ip enable

By default, IEEE 802.1X and MAB authentication do not carry static IP addresses in authentication and accounting packets.

- Recording Debugging Information to a File

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 IEEE 802.1X authentication function is enabled by default.

(4) (Optional) Configure the number of Request/Identity packets to be sent by a port added to a failed VLAN.

dot1x auto-req fail-vlan-pkt-num *packet-number*

The function of sending Request/Identity packets by a port added to a failed VLAN is disabled by default.

When both IEEE 802.1X authentication and MAB are enabled, a port may be added to a failed VLAN if MAB fails. Some clients cannot initiate IEEE 802.1X authentication actively. For this, you can configure this function to send Request/Identity packets to the clients to trigger authentication.

(5) (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.

(6) (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.

(7) (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 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.

1.13.13 Enabling Perception-free Migration Across VLANs for 802.1X Users

1. Overview

This function enables and controls migration of 802.1X users across VLANs in perception-free mode.

When this function is disabled, user migration across VLANs is not allowed if only the VLAN ID of the users changes. If both the VLAN ID and interface change, migration across VLANs is allowed for users such as new users getting online, old users staying online, and users with two user entries on their devices.

After this function is enabled, migration across VLANs is allowed for users such as new users getting online, offline old users, and users with one user entry on their devices.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable perception-free migration across VLANs for 802.1X users.

dot1x vlan-move permit

Perception-free migration across VLANs is disabled for 802.1X users by default.

1.13.14 Configuring the Function of Instantly Sending Accounting Update Packets Upon IP Address Changes of 802.1X Authenticated Users

1. Overview

After this function is enabled, the device instantly sends accounting update packets when the IP address of an 802.1X authenticated user changes.

2. Restrictions and Guidelines

- This function can be enabled only after the IEEE802.1X authentication function is enabled.
- This function must be configured when the server requires instant accounting update upon IP address changes.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of instantly sending accounting update packets upon IP address changes of 802.1X authenticated users.

dot1x acct-update ip-addr-change instant

The function of instantly sending accounting update packets upon IP address changes of 802.1X authenticated users is disabled by default.

1.13.15 Converting User Names into TEXT Format

1. Overview

This function converts user names into TEXT format.

When the user names used by clients are of the string type, the user name length may contain the ending space. Running this command can recalculate the user name length.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of converting user names into TEXT format.

dot1x user-name format text

By default, user names are not converted into TEXT format.

1.13.16 Compatible with Third-Party Clients

1. Overview

The device is compatible with the third-party clients that encapsulate reply-msg messages in the format of type (1 byte, fixed as 09), length (1 byte, length of value), and value (character string in reply-msg).

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the device to be compatible with third-party clients.

dot1x not-private-supplicant compatible

By default, the device is not compatible with third-party clients.

1.13.17 Configuring the Function of Carrying Static IP Addresses in Authentication and Accounting Packets for IEEE 802.1X and MAB

1. Overview

After this function is configured, when the device receives an ARP packet sent by a terminal with a static IP address, the device reports the static IP address carried in the IEEE 802.1X and MAB authentication and accounting packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the function of carrying static IP addresses in IEEE 802.1X and MAB authentication and accounting packets.

dot1x get-static-ip enable

By default, IEEE 802.1X and MAB authentication do not carry static IP addresses in authentication and accounting packets.

1.13.18 Recording Debugging Information to a File

1. Overview

To locate faults on a network, you can enable the function of recording debugging information to a file to avoid login freeze or service impact caused by a large amount of debugging information.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of recording debugging information to a file.

dot1x dbg-to-file

The function of recording debugging information to a file is disabled by default.

1.14 Monitoring

Run the **show** command to check the configuration.

Run the **dot1x** command to restore global configuration.

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 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.
show dot1x authmng [**mab**] **abnormal** [**auth** | **offline** | **reauth**]	Displays all authentication records of 802.1X or MAB authentication in global configuration mode.
show dot1x authmng [**mab**] **statistic** [**auth-detail** | **fail** | **offline-detail** | **reauth-detail**]	Displays global static statistics of IEEE 802.1X or MAB authentication.
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 max-req	Displays the maximum retransmission count of Request/Challenge packets.
show dot1x multi-mab quiet user	Displays the list of quiet users for multi-MAB authentication.
show dot1x port-control [**interface** *interface-type interface-numbe*r]	Displays information about controlled ports.
show dot1x private-supplicant-only	Displays the status of the non-Ruijie client filtering function.
show dot1x probe-timer	Displays client detection parameters.
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 summary	Displays entries of authenticated users.
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-address*	Displays details about a user with a specific MAC address.

Command	Purpose
show dot1x user name *user-name*	Displays details about a user with a specific username.
show dot1x user diag *mac-address*	Displays the configuration of the user track recording function.
show dot1x user diag all	Display track records of all users.
show dot1x user diag mac	Displays track records of the specified user.
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.
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

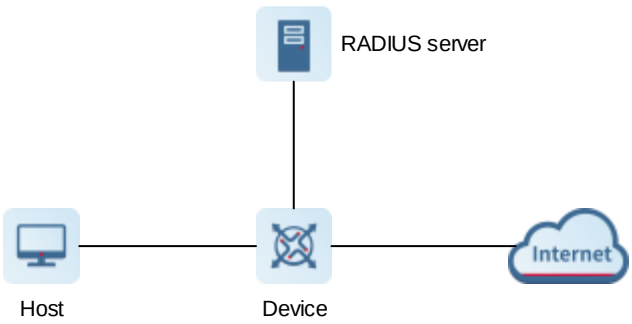
1.15.1 Configuring IEEE 802.1X Authentication

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 **Abc123456** on the RADIUS server. (The configuration is omitted here. For the configuration of the RADIUS server, see the RADIUS server configuration.)

(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.

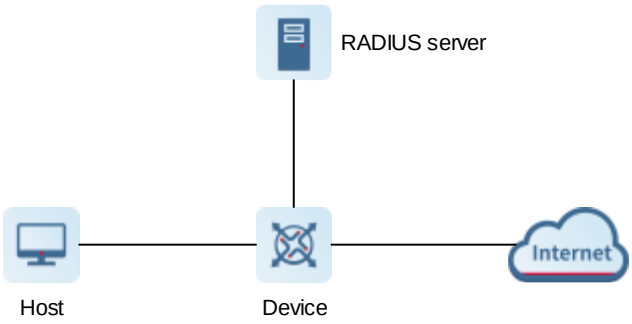
1.15.2 Configuring the IP Authorization Mode

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.

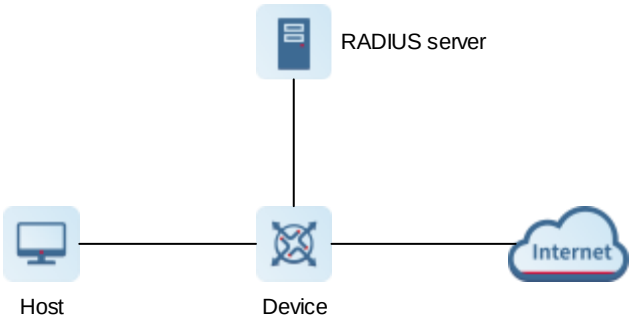
1.15.3 Configuring Multi-user MAB

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.

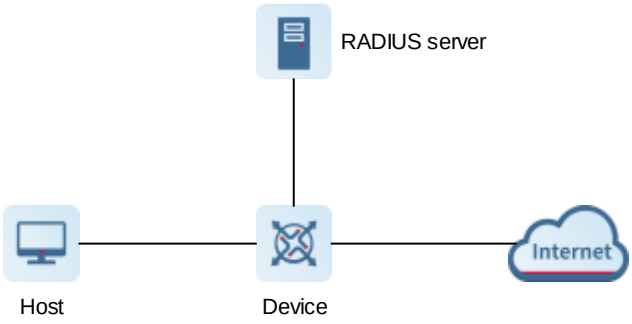
1.15.4 Configuring IAB

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.

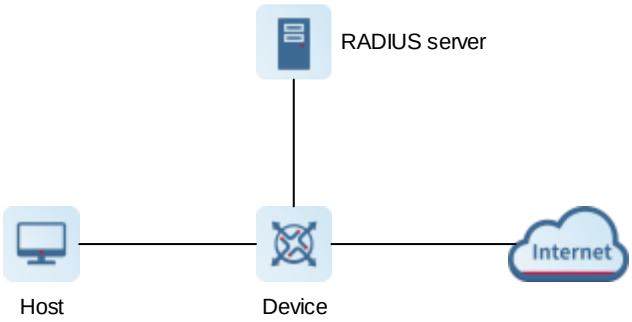
1.15.5 Configuring Automatic Dynamic VLAN Redirection

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.

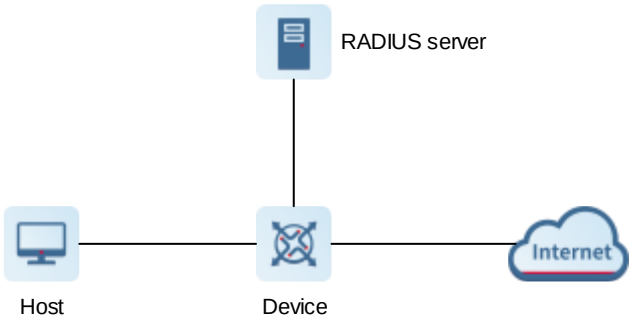
1.15.6 Configuring Guest VLAN

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.

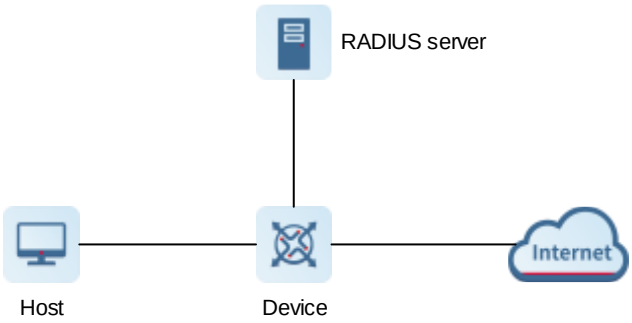
1.15.7 Configuring Failed VLAN

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 10
1.2 Restrictions and Guidelines 10
1.3 Configuration Task Summary 10
1.4 Configuring Ruijie First-Generation Web Authentication 11
1.4.1 Overview 11
1.4.2 Restrictions and Guidelines 11
1.4.3 Prerequisites 12
1.4.4 Procedure 12
1.5 Configuring Ruijie Second-Generation Web Authentication 14
1.5.1 Overview 14
1.5.2 Restrictions and Guidelines 14
1.5.3 Prerequisites 14
1.5.4 Procedure 14
1.6 Configuring ClearPass Authentication 16
1.6.1 Overview 16
1.6.2 Restrictions and Guidelines 16
1.6.3 Prerequisites 16
1.6.4 Procedure 16

1.7 Configuring App-based Authentication 19
1.7.1 Overview 19
1.7.2 Restrictions and Guidelines 19
1.7.3 Procedure 19
1.8 Configuring an Authentication Method List 20
1.8.1 Overview 20
1.8.2 Restrictions and Guidelines 20
1.8.3 Procedure 20
1.9 Configuring an Accounting Method List 21
1.9.1 Overview 21
1.9.2 Restrictions and Guidelines 21
1.9.3 Procedure 21
1.10 Configuring the Portal Communication Destination Port 21
1.10.1 Overview 21
1.10.2 Restrictions and Guidelines 21
1.10.3 Procedure 22
1.11 Configuring the Binding Mode 22
1.11.1 Overview 22
1.11.2 Restrictions and Guidelines 22
1.11.3 Procedure 22
1.12 Configuring the Redirection HTTP Port 23
1.12.1 Overview 23
1.12.2 Restrictions and Guidelines 23
1.12.3 Procedure 23

1.13 Configuring the Redirection Connection Timeout Time 23
1.13.1 Overview 23
1.13.2 Procedure 23
1.14 Configuring Portal Detection 24
1.14.1 Overview 24
1.14.2 Restrictions and Guidelines 24
1.14.3 Procedure 24
1.15 Configuring Portal Escape 24
1.15.1 Overview 24
1.15.2 Restrictions and Guidelines 25
1.15.3 Procedure 25
1.16 Configuring the Portal Communication Source Port 25
1.16.1 Overview 25
1.16.2 Restrictions and Guidelines 25
1.16.3 Procedure 25
1.17 Disabling Portal Specification Extension 25
1.17.1 Overview 25
1.17.2 Restrictions and Guidelines 26
1.17.3 Procedure 26
1.18 Configuring Transparent Transmission of RADIUS Private Attributes 26
1.18.1 Overview 26
1.18.2 Restrictions and Guidelines 26
1.18.3 Procedure 26
1.19 Configuring the Authentication-Free Network Resource Range 27

1.19.1 Overview 27
1.19.2 Restrictions and Guidelines 27
1.19.3 Procedure 27
1.20 Configuring a Straight-through ARP Resource Range 27
1.20.1 Overview 27
1.20.2 Restrictions and Guidelines 27
1.20.3 Procedure 28
1.21 Configuring an Authentication-Exempted User Range 28
1.21.1 Overview 28
1.21.2 Restrictions and Guidelines 28
1.21.3 Procedure 28
1.22 Configuring Logging of the Web Authentication Module 29
1.22.1 Overview 29
1.22.2 Restrictions and Guidelines 29
1.22.3 Procedure 29
1.23 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users 29
1.23.1 Overview 29
1.23.2 Restrictions and Guidelines 29
1.23.3 Procedure 29
1.24 Configuring the Interval for Updating Online User Information 30
1.24.1 Overview 30
1.24.2 Restrictions and Guidelines 30
1.24.3 Procedure 30
1.25 Enabling DHCP Address Check 30

1.25.1 Overview 30
1.25.2 Restrictions and Guidelines 30
1.25.3 Configuration Tasks 31
1.25.4 Configuring Global DHCP Address Check 31
1.25.5 Configuring DHCP Address Check on an Interface 31
1.26 Configuring an Address Whitelist 32
1.26.1 Overview 32
1.26.2 Restrictions and Guidelines 32
1.26.3 Procedure 32
1.27 Configuring VLAN-based Authentication on a Port 32
1.27.1 Overview 32
1.27.2 Restrictions and Guidelines 32
1.27.3 Procedure 32
1.28 Configuring the Authenticated User Logout Delay on a Port 33
1.28.1 Overview 33
1.28.2 Restrictions and Guidelines 33
1.28.3 Procedure 33
1.29 Enabling RADIUS Server Escape 33
1.29.1 Overview 33
1.29.2 Restrictions and Guidelines 33
1.29.3 Procedure 33
1.30 Configuring DHCP Server Detection 34
1.30.1 Overview 34
1.30.2 Restrictions and Guidelines 34

1.30.3 Procedure....34
1.31 Configuring Uniqueness Check of Portal Authentication Accounts....34
1.31.1 Overview....34
1.31.2 Procedure....34
1.32 Enabling Automatic Adding of Domain Information After Usernames....35
1.32.1 Overview....35
1.32.2 Restrictions and Guidelines....35
1.32.3 Procedure....35
1.33 Configuring Seamless Migration of Web Authentication Users....35
1.33.1 Overview....35
1.33.2 Restrictions and Guidelines....36
1.33.3 Procedure....36
1.34 Configuring HTTPS Certificate Import....36
1.34.1 Overview....36
1.34.2 Procedure....36
1.35 Enabling Adding the Authentication Page to Favorite....37
1.35.1 Overview....37
1.35.2 Restrictions and Guidelines....37
1.35.3 Procedure....37
1.36 Configuring a Template Mapping Method....37
1.36.1 Overview....37
1.36.2 Restrictions and Guidelines....37
1.36.3 Procedure....37
1.37 Monitoring....38

1.38 Configuration Examples....39

1.38.1 Configuring First-Generation Web Authentication....39

1.38.2 Configuring Second-Generation Web Authentication....42

1.38.3 Configuring ClearPass Authentication....45

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.

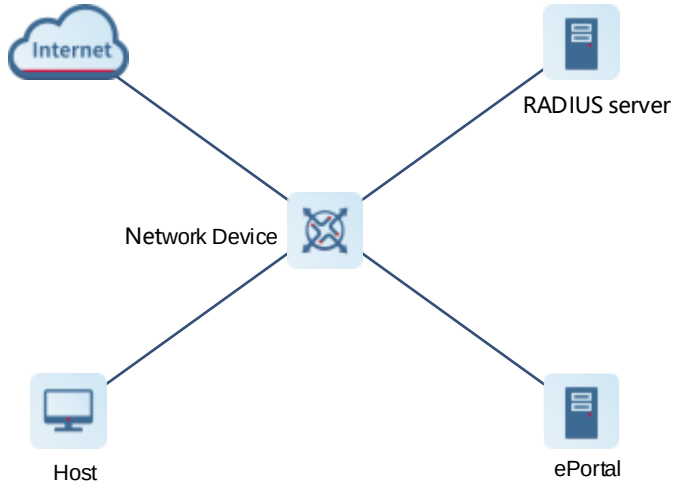
- HTTP redirection

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

Authentication Solution		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.

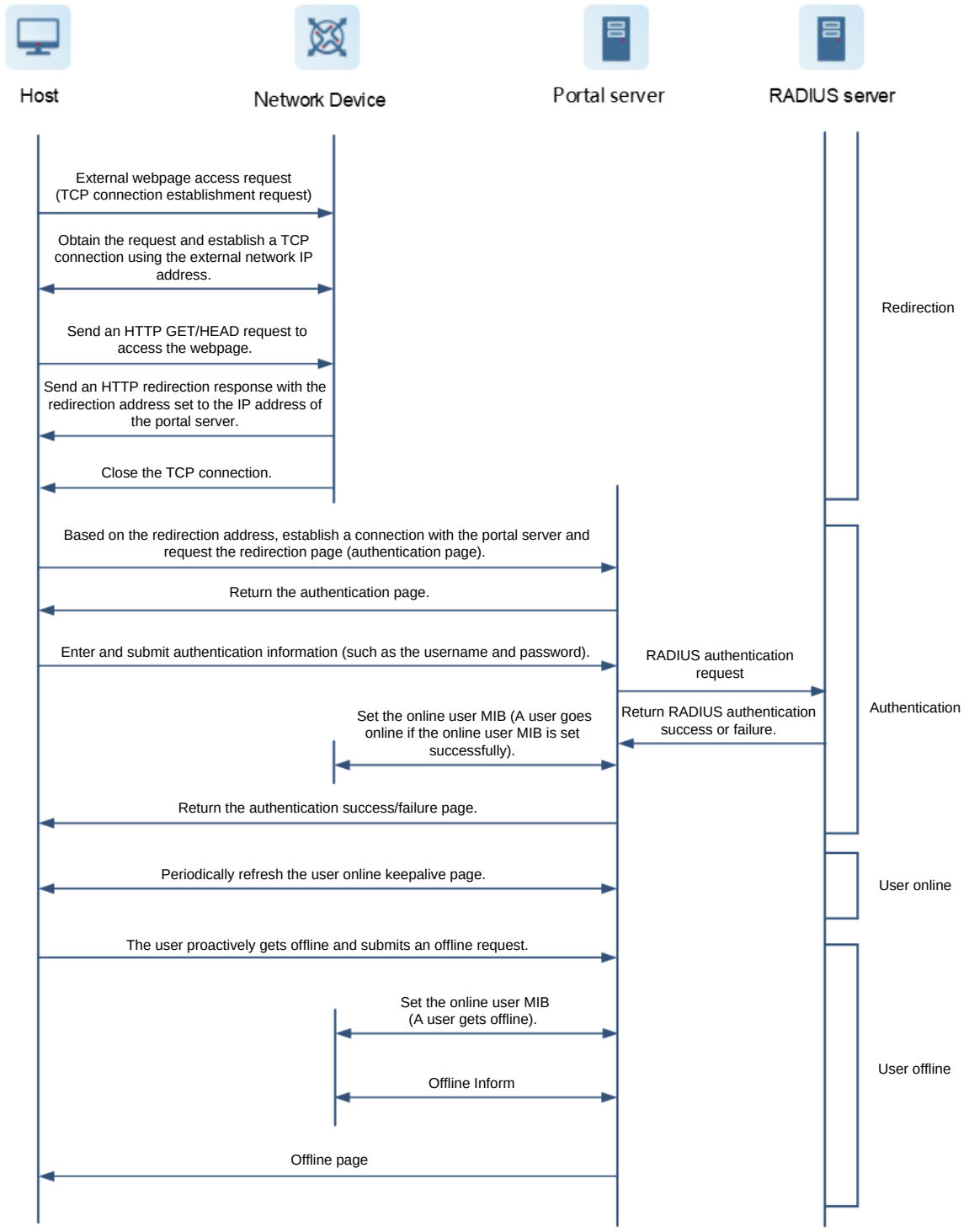
Note

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.

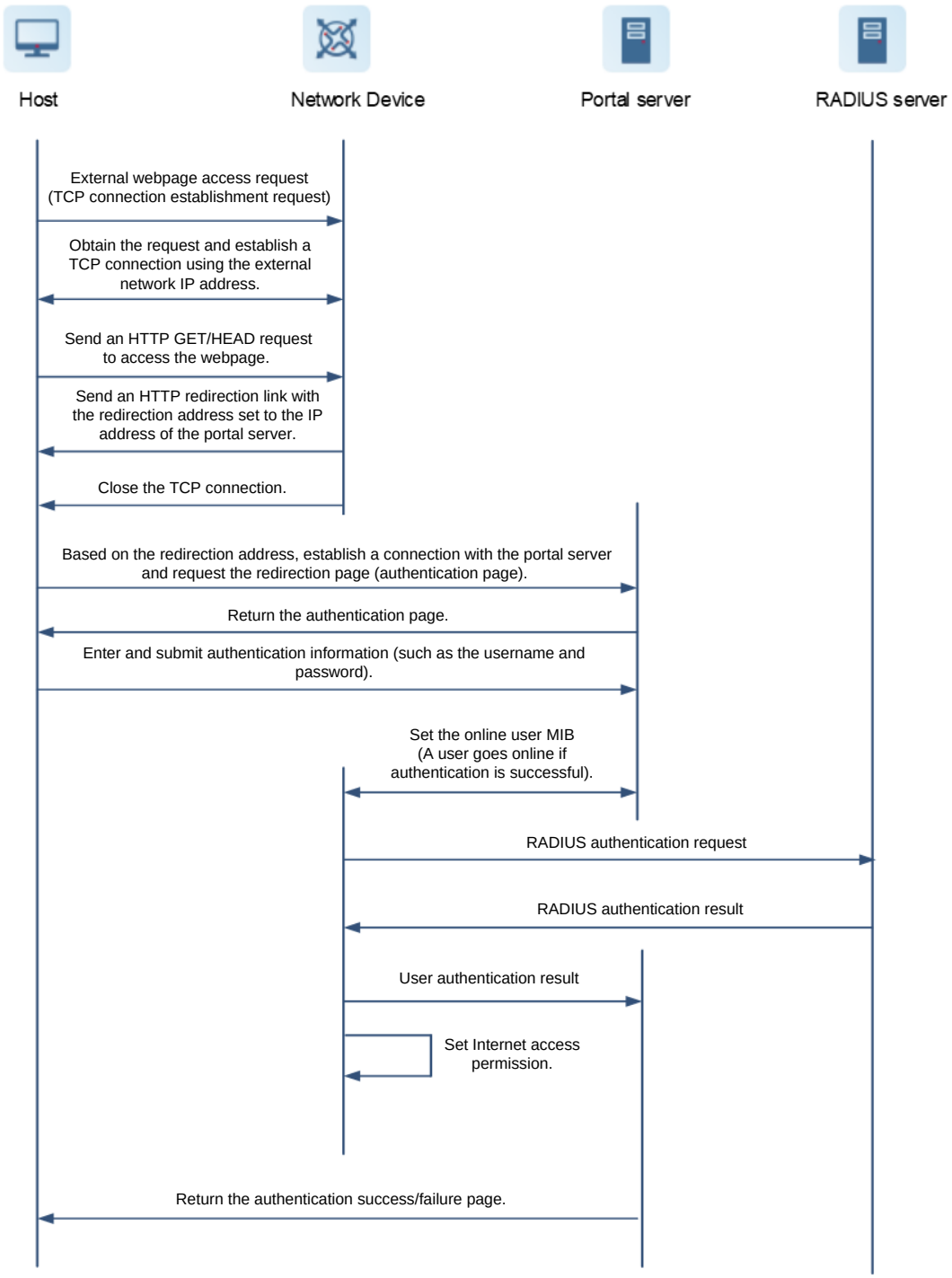
(4) User offline

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. ClearPass Authentication

- Roles in web authentication
  - Authentication client

    In most cases, an authentication client is a browser running the HTTP protocol. When a user accesses the network from the browser, the browser initiates an HTTP request.

  - Network device

    In most cases, a network device in ClearPass authentication is an access layer device (such as the wireless AP on the wireless network) in the network topology, which is directly connected to user terminal. The web authentication function must be enabled on the network device. This device controls users' network access permissions, accepts the token verification requests from authentication clients or permits network access requests, and verifies the token information of the Portal server.

  - Portal server

    The Portal server is used to provide the authentication page and related operations of web authentication. The Portal server accepts an HTTP-based authentication request from an authentication client, extracts account information from the request, authenticates the information in the background, and forwards the authentication result to the network device through the authentication client. After the network device completes verification, the authentication client is redirected to the relevant page of the Portal server.

  - Authentication server

    The authentication server is used to provide the user authentication service through the specific protocol (such as the RADIUS protocol) negotiated by the Portal server and the authentication server.

- ClearPass authentication process

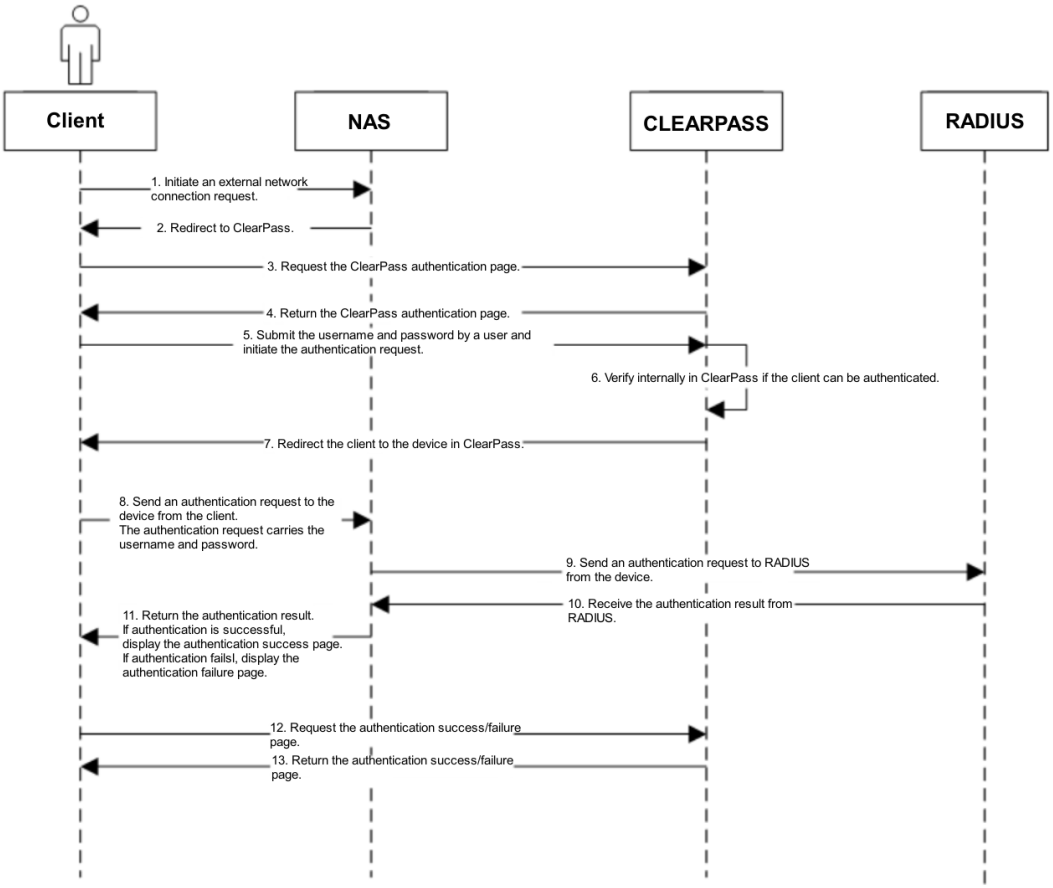
  a Before authentication, the device blocks all the HTTP requests from the user not authenticated, directs the user to the Portal server, and pops an authentication page on the user browser.

  b During the authentication process, the user enters the authentication information (such as the username, password, and verification code) on the authentication page to exchange with the Portal server.

c The Portal server verifies the validity of user information in the background. If authentication fails, the server returns the authentication failure page to the client. If authentication succeeds, the server redirects the client to the network device.

d After the network device receives a request from the authentication client, it initiates verification to the Portal server and redirects the client to the relevant page of the Portal server based on the verification result.

Figure 1-4 Flowchart of ClearPass Authentication



- User logout process

  User logout occurs in either of the following cases: passive user logout by the device when the maximum user online duration is reached, the traffic is used up, or the link is disconnected and active user logout when the user clicks the Logout button.

  a The user actively clicks the Logout button on the page and confirms to log out. A logout request is sent to both the Portal server and the network device. (The request may not be sent simultaneously, depending on the implementation of the Portal server.)

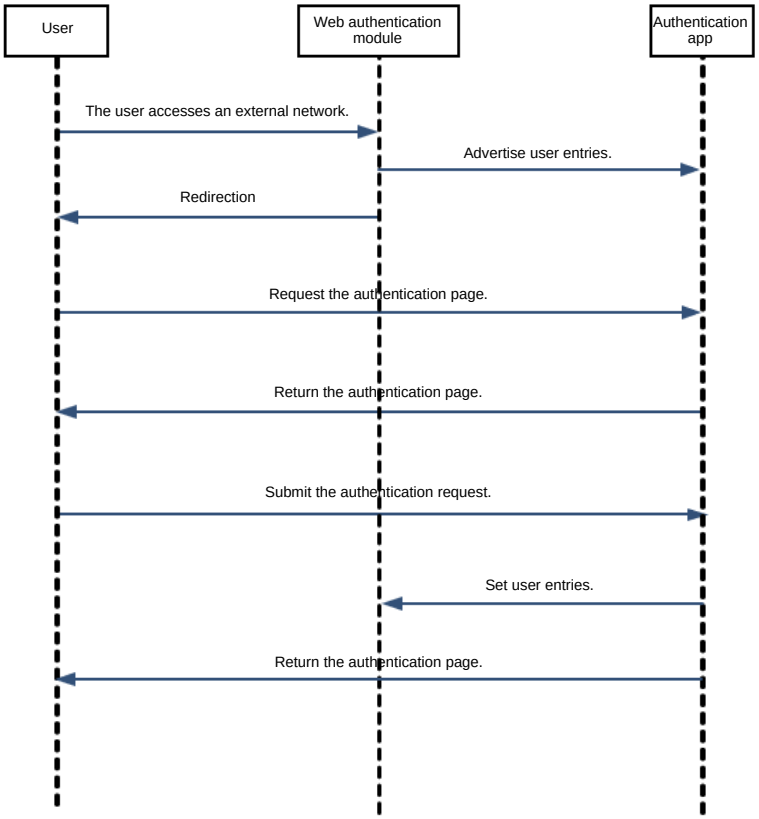
  b The device logs the user out when it detects that the user has low traffic. This method depends on the configured low traffic detection parameters.

6. 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 1-5 Flowchart of App-based Web Authentication



As shown in Figure 1-5, 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

- RFC 1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC 2068: Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2818: HTTP Over TLS
- RFC 1157: Simple Network Management Protocol (SNMP)
- RFC 2865: Remote Authentication Dial In User Service (RADIUS)
- RFC 2866: RADIUS Accounting
- RFC 3576: 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*.

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 ClearPass Authentication
- ClearPass authentication is disabled on the interface by default.
- 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
- Configuring Transparent Transmission of RADIUS Private Attributes

(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
- Configuring Seamless Migration of Web Authentication Users

(6) (Optional) Configure other functions. Perform the following optional configuration tasks as required.

- 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*.
- 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 RADIUS server configuration.

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 [*ipv4-address* | **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 (Optional) 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** { *ipv4-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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 RADIUS server configuration.

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 [*ipv4-address* | **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 (Optional) 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(12) Enable second-generation web authentication on a port.

web-auth enable eportalv2

1.6 Configuring ClearPass Authentication

1.6.1 Overview

The ClearPass server can function as the Portal server to connect to the web authentication component, directing authenticated users to the authentication page for authentication.

1.6.2 Restrictions and Guidelines

- The device can only connect to the ClearPass server of Aruba that functions as the Portal server for ClearPass authentication.
- When you configure the ClearPass authentication service, you need to configure a ClearPass authentication template, enable the local HTTP server, and configure the IP addresses of the ClearPass server and the NAS device where the authentication service resides as authentication-free resources.
- The ClearPass authentication server can exchange only HTTP packets with the ClearPass server.

1.6.3 Prerequisites

- Valid user information is configured on the RADIUS server. For details about user information configuration on the RADIUS server, see the RADIUS server configuration.
- Portal authentication services are configured on the ClearPass server. For detailed configuration, see the ClearPass server configuration.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the AAA security services.

aaa new-model

The AAA security services are disabled by default.

When ClearPass authentication is used, the device is responsible for initiating authentication to the server. The detailed functions are implemented by the AAA module.

(4) Configure the address, port number, and key for a 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 address, port number, or key is configured for a RADIUS server by default. The default authentication port number is 1812 and the default accounting port number is 1813.

User account information is stored on the RADIUS server. The device needs to connect to the RADIUS server to confirm user identity.

(5) Configure a ClearPass authentication method list.

aaa authentication cpweb { **default** | *list-name* } { [**group** *group-name*]&<1-4> | **group radius** | **local** | **none** } *

No ClearPass authentication method list is configured by default.

The authentication method list associates the web authentication request with the RADIUS server. The device selects an authentication method and the corresponding server based on the 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 network accounting function is disabled by default.

The accounting method is used to associate the accounting method with a server. Web authentication needs the accounting feature to record user information or fees.

(7) Create a ClearPass authentication profile and enter the ClearPass authentication template configuration mode.

web-auth template cpweb

(8) Configure web authentication template parameters.

a Configure an IP address and a VRF instance for the Portal server.

ip [*ipv4-address*]

No IP address is configured for the Portal server by default.

b Configure a page address for the Portal server.

url *url-string*

No page address is configured for the Portal server by default.

c (Optional) Configure the URL format for redirection packets.

fmt { **custom** | **clearpass** }

Redirection packets use the ClearPass URL format by default.

d Configure a method used by the device to parse authentication requests.

http-method post [**init-url-key** *urlkey-string* | **password-encrypt** { **none** | **uam** } | **password-key** *pswkey-string* | **username-key** *usrkey-string*] *

By default, the authentication packet is parsed based on the username, password, and URL parameter name. The password is not encrypted.

e Configure the encapsulation format of redirection packets.

redirect { **http** | **js** }

The JS format is used for redirection packets by default.

f Configure the response mode after successful authentication.

login-success response { **redirect-init-url** [**reset-url** *def-string*] | **msg** *msg-string* | **redirect-url** *url-string* }

The authentication success page is displayed after successful user authentication by default.

g Configure the response mode after failed authentication.

login-fail response { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] | **msg** *msg-string* }

The user is redirected to the authentication page after failed authentication by default.

h Pop up the active logout page after successful authentication. (This command takes effect only when a redirection URL for successful authentication is configured.)

logout-popup-window

This function is disabled by default.

(9) Configure a communication IP address for the HTTP server.

web-auth auth-server ip ipv4-address

No communication IP address is configured for the HTTP server by default.

(10) Configure a communication port for the HTTP server.

web-auth auth-server http [**port** *port*]

No communication port is configured for the HTTP server by default.

(11) Exit to the global configuration mode.

exit

(12) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *interface-number*

(13) Enable ClearPass authentication on the interface.

web-auth enable cpweb

ClearPass authentication is disabled on the interface by default.

1.7 Configuring App-based Authentication

1.7.1 Overview

The authentication app can interwork with the web authentication component to redirect unauthenticated users to the authentication page for authentication.

1.7.2 Restrictions and Guidelines

In template configuration mode, the authentication app name must be correctly configured.

1.7.3 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 [*ipv4-address* | **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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(8) Enable app-based authentication on a port.

web-auth enable appauth

1.8 Configuring an Authentication Method List

1.8.1 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.

1.8.2 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.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the second-generation 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.

1.9 Configuring an Accounting Method List

1.9.1 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.

1.9.2 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.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the second-generation 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.

1.10 Configuring the Portal Communication Destination Port

1.10.1 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.

1.10.2 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.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the second-generation web authentication template configuration mode or app-based 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.

1.11 Configuring the Binding Mode

1.11.1 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.

1.11.2 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).

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the 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.

1.12 Configuring the Redirection HTTP Port

1.12.1 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.

1.12.2 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.

1.12.3 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.

1.13 Configuring the Redirection Connection Timeout Time

1.13.1 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.

1.13.2 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.

1.14 Configuring Portal Detection

1.14.1 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.

1.14.2 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.

1.14.3 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.

1.15 Configuring Portal Escape

1.15.1 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.

1.15.2 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.

1.15.3 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.

1.16 Configuring the Portal Communication Source Port

1.16.1 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.

1.16.2 Restrictions and Guidelines

Only one portal communication source port can be configured.

1.16.3 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.

1.17 Disabling Portal Specification Extension

1.17.1 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.

1.17.2 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.

1.17.3 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.

1.18 Configuring Transparent Transmission of RADIUS Private Attributes

1.18.1 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.

1.18.2 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.

1.18.3 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.

1.19 Configuring the Authentication-Free Network Resource Range

1.19.1 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.

1.19.2 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.

1.19.3 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.

1.20 Configuring a Straight-through ARP Resource Range

1.20.1 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.

1.20.2 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.

1.20.3 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.

1.21 Configuring an Authentication-Exempted User Range

1.21.1 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.

1.21.2 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.

1.21.3 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.

1.22 Configuring Logging of the Web Authentication Module

1.22.1 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.

1.22.2 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.

1.22.3 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.

1.23 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users

1.23.1 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.

1.23.2 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.

1.23.3 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.

1.24 Configuring the Interval for Updating Online User Information

1.24.1 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.

1.24.2 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.

1.24.3 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.

1.25 Enabling DHCP Address Check

1.25.1 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.

1.25.2 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.

1.25.3 Configuration Tasks

The following DHCP address check configuration tasks are optional. Perform the configuration tasks as required.

- Configuring Global DHCP Address Check
- Configuring DHCP Address Check on an Interface

1.25.4 Configuring Global DHCP Address Check

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP address check globally.

web-auth dhcp-check

DHCP address check is disabled globally by default.

1.25.5 Configuring DHCP Address Check 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 *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

interface aggregateport *interface-number*

(4) Enable DHCP address check on an interface. The following configuration tasks are mutually exclusive. Perform one of the tasks as required.

- Enable DHCP address check for all VLANs on an interface.

web-auth dhcp-check

- Enable DHCP address check for a specified VLAN on an interface.

web-auth dhcp-check vlan *vlan-list*

- Enable DHCP address check for VLANs except the specified VLAN on an interface by running the following commands in sequence.

web-auth dhcp-check

no web-auth dhcp-check vlan *vlan-list*

DHCP address check is disabled for all VLANs on an interface by default.

If both the **web-auth dhcp-check** and **web-auth dhcp-check vlan** commands are configured, DHCP address check is enabled for all VLANs on the interface.

(5) (Optional) Disable DHCP address check on a VLAN.

web-auth dhcp-check disable

DHCP address check is disabled on an interface by default.

The **web-auth dhcp-check disable** command and the **no web-auth dhcp-check** command on an interface have the same configuration effect. The later configuration on the interface takes effect.

1.26 Configuring an Address Whitelist

1.26.1 Overview

After an address whitelist is configured, users can access some network resources before authentication.

1.26.2 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.

1.26.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an address whitelist.

web-auth acl [**vrf** *vrf-name*] **white-url** *white-url-name*

No whitelist is configured by default.

1.27 Configuring VLAN-based Authentication on a Port

1.27.1 Overview

After VLAN-based authentication is configured on a port, only the user hosts in the configured VLAN can initiate web authentication.

1.27.2 Restrictions and Guidelines

When this function is configured, multiple VLANs can be specified.

1.27.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.28 Configuring the Authenticated User Logout Delay on a Port

1.28.1 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.

1.28.2 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.

1.28.3 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.

1.29 Enabling RADIUS Server Escape

1.29.1 Overview

After the RADIUS server escape function is configured, users can still perform authentication to access the Internet when the RADIUS server fails.

1.29.2 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*.

1.29.3 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.

1.30 Configuring DHCP Server Detection

1.30.1 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.

1.30.2 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.

1.30.3 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.

1.31 Configuring Uniqueness Check of Portal Authentication Accounts

1.31.1 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.

1.31.2 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.

1.32 Enabling Automatic Adding of Domain Information After Usernames

1.32.1 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.

1.32.2 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.

1.32.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the 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.

1.33 Configuring Seamless Migration of Web Authentication Users

1.33.1 Overview

A migration policy is used by the authentication component when a web authentication user performs migration on an interface or VLAN. After the seamless migration function is enabled, users who pass web authentication can be migrated without being logged out.

1.33.2 Restrictions and Guidelines

- Seamless user migration takes effect only after migration of authentication users is enabled through the **station-move permit** command. For details, see "Configuring SCC".

1.33.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the seamless migration function for web-authenticated users.

web-auth station-move auto

The MAB migration function is disabled by default.

(4) (Optional) Configure the function of immediately updating accounting information after a user is migrated.

web-auth station-move info-update

The function of immediately updating accounting information after seamless migration is disabled by default, that is, accounting information is not updated immediately after seamless migration, but is updated by accounting packets sent based on the accounting interval.

1.34 Configuring HTTPS Certificate Import

1.34.1 Overview

HTTPS encrypts data for transmission and ensures transmission security using certificates. Before enabling the HTTPS server function, you need to import an available certificate.

To configure HTTPS certificate import, first upload available HTTPS certificates and key files to the device and then apply the HTTPS certificate and key files.

Two types of HTTPS certificates can be imported: HTTPS redirection certificate and HTTPS certificate of ClearPass authentication.

1.34.2 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) Enter the global configuration mode.

configure terminal

(4) Apply the HTTPS certificate and key files.

web-auth ssl-policy https-redirect

No HTTPS certificate or key file is applied by default.

1.35 Enabling Adding the Authentication Page to Favorite

1.35.1 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.

1.35.2 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.

1.35.3 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.

1.36 Configuring a Template Mapping Method

1.36.1 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.

1.36.2 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.

1.36.3 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

1.37 Monitoring

Run the **show** commands to check the configuration.

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

Caution

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

Table 1-2 Monitoring

Command	Purpose
show web-auth acl { **white-url** }	Displays allowlist configurations.
show web-auth authhmng [**statistic** | **abnormal**]	Displays the web authentication data.
show web-auth auth-server	Displays parameters of the local HTTP server.
show web-auth parameter	Displays basic parameter configurations for web authentication.
show web-auth control	Displays authentication control configuration.
show web-auth dhcp-bind-info	Displays the DHCP information of users in the web authentication buffer. The information source is DHCP snooping.
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.

Command	Purpose
show web-auth rdport	Displays the TCP interception port.
show web-auth syslog [**ip** *ipv4-addres* | ***name*** *name* | ***mac*** *mac-address*]	Displays user online and offline records.
show web-auth template	Displays portal server configurations.
show web-auth capability	Displays Web authentication capability.
show web-auth ssl-policy info	Displays SSL certificate information.
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 blacklist and 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 user offline.
debug web-auth all	Debugs web authentication.

1.38 Configuration Examples

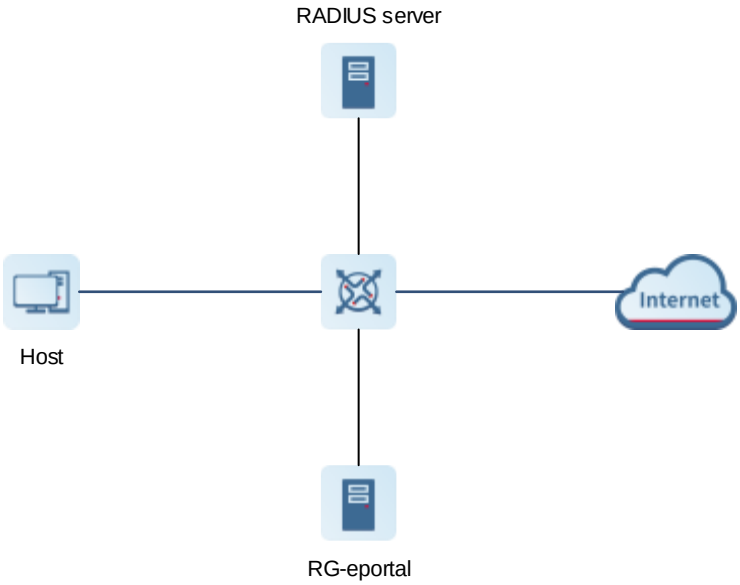
1.38.1 Configuring First-Generation Web Authentication

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 1-6 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)# interface 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.

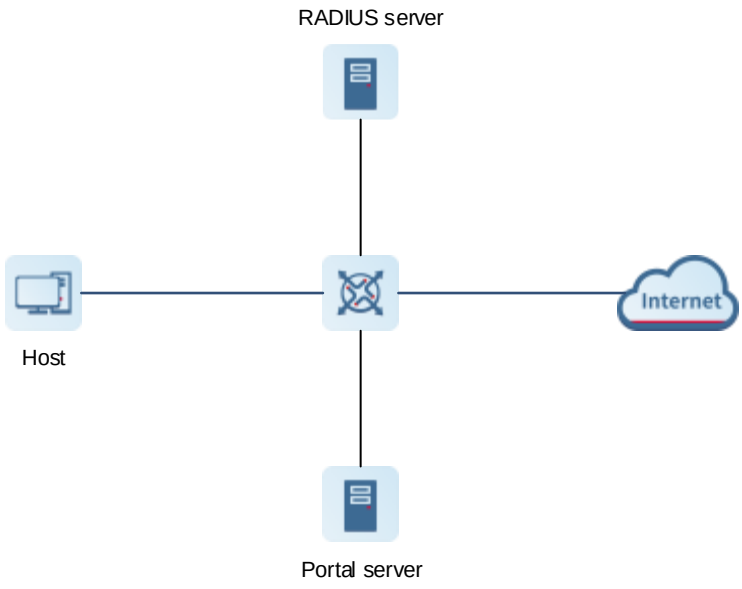
1.38.2 Configuring Second-Generation Web Authentication

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 1-7 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)# interface 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.

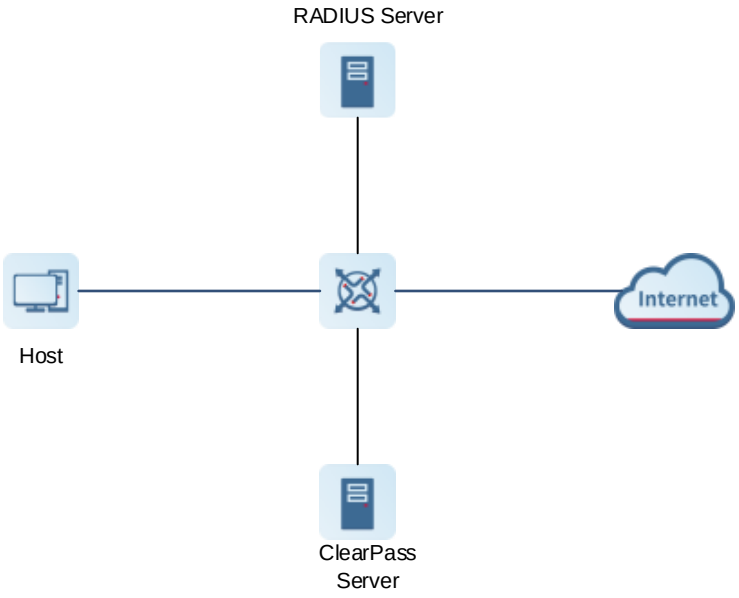
1.38.3 Configuring ClearPass Authentication

1. Requirements

The device functions as the network access server to provide ClearPass authentication to access users on a specific port. Users need to pass authentication using valid account and password before they can access the network.

2. Topology

Figure 1-8 Topology of ClearPass Authentication



3. Notes

- Configure the ClearPass server as the Portal server to support ClearPass authentication.
- Configure the RADIUS server to support ClearPass Web authentication.
- Configure a ClearPass web authentication template and specify parameters such as the Portal server IP address and redirection page.
- Enable the ClearPass authentication service on the port of the device.

4. Procedure

(1) Configure the ClearPass server and the RADIUS server to support ClearPass authentication. For details, see the corresponding configuration guide.

(2) Configure a ClearPass web authentication template and set the Portal server IP address to 172.29.121.53 and the redirection URL to http://172.29.121.53/ruijie.php. In the URL, ruijie is the web template name configured on the ClearPass server.

```
Device> enable
Device# configure terminal
Device(config)# web-auth template cpweb
Device(config.tmplt.cpweb)# ip 172.29.121.53
Device(config.tmplt.cpweb)# url http://172.29.121.53/ruijie.php
Device(config.tmplt.cpweb)# exit
```

(3) Configure the communication IP address and port number of the HTTP server and the URL used to initiate authentication.

```
Device(config)# web-auth auth-server http port 8082
Device(config)# web-auth auth-server ip 172.20.74.159
```

(4) Configure the addresses for the Portal server and the local HTTP server.

```
Device(config)# http redirect direct-site 192.168.197.79
Device(config)# http redirect direct-site 172.20.74.159
```

(5) Enable ClearPass authentication on GigabitEthernetwork 0/2 and GigabitEthernetwork 0/3.

```
Device(config)# interface range gigabitEthernetwork 0/2-3
Device(config-if-range)# web-auth enable cpweb
```

(6) Configure AAA authentication and accounting services.

```
Device(config)# aaa new-model
Device(config)# aaa authentication cpweb default group radius
Device(config)# aaa accounting network default start-stop group radius
```

(7) Configure the RADIUS service.

```
Device(config)# radius-server host 172.26.147.194 key test
```

5. Verification

Check whether ClearPass authentication takes effect on GigabitEthernetwork 0/2 and GigabitEthernetwork 0/3.

```
Device# display web-auth control
 Port                   Control  Server Name    Online User Count Arp-detect Vlan
Control Range
 ------------------------- -------- -------------------------------
----------------- ----------
 GigabitEthernetwork 0/2      On      cpweb          0              Off
 GigabitEthernetwork 0/3      On      cpweb          0              Off
```

Check whether the parameters in the ClearPass web authentication template are correct.

```
Device# display web-auth template
Webauth Template Settings:
-------------------------------------------------------------
```

```
 Name:          cpweb
 Type:          cpweb
 Ip:            172.29.121.53
 Url:           http://172.29.121.53/ruijie.php
 Logout-popup:   off
 Login-success:  redirect-init-url
 Login-fail:    show-msg
```

Check whether terminals connecting to GigabitEthernetwork 0/2 and GigabitEthernetwork 0/3 of the device are redirected to http://172.29.121.53/ruijie.php for identity authentication when they access any web page. The terminals can access the network only after they pass identity authentication.

6. Configuration Files

```
!
web-auth template cpweb
 ip 172.29.121.53
 url http://172.29.121.53/ruijie.php
!
aaa new-model
!
aaa authentication cpweb default group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.26.147.194 key 7 $10$3ed$f/3upXnVEhd9$
!
web-auth auth-server http port 8082
web-auth auth-server ip 172.20.74.159
http redirect direct-site 192.168.197.79
http redirect direct-site 172.20.74.159
!
interface GigabitEthernetwork 0/2
 web-auth enable cpweb
!
interface GigabitEthernetwork 0/3
 web-auth enable cpweb
!
```

7. Common Errors

- The NAS device is not registered on the ClearPass server, causing authentication and login errors.
- The IP address of the Portal server and the IP address of the NAS device are not permitted, causing login errors.

Contents

1 Configuring 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 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *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.

Caution

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.

After the strong password detection function is enabled, the password must meet the following conditions:

- The password cannot contain the account string. The case of the password is ignored during detection.
- If the special character detection function is disabled, the password must contain digits, lowercase letters, and uppercase letters.
- If special character detection is enabled, the password must contain at least three of the following types: digits, lowercase letters, uppercase letters, and special characters.

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 enabled 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

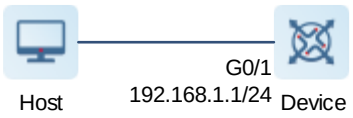
To ensure password complexity, you can configure password policies on a device to limit users' passwords.

Password security requirements are as follows:

- A password must be a string of at least eight characters.
- A password cannot contain the account string.
- A password must contain at least three types of the following: digits, uppercase letters, lowercase letters, and special characters.
- 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# 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:  Enabled
```

1.12.6 Configuration Files

```
!
password policy life-cycle 90
password policy no-repeat-times 3
password policy printable-character-check
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....4
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....8
1.3.10 Configuring IP Address Blocking....8
1.3.11 Disconnecting an SSH Client Connection....9
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 SFTP Server....10

1.5.1 Overview 10
1.5.2 Procedure 10
1.6 Configuring SSH Client 10
1.6.1 Overview 10
1.6.2 Configuration Tasks 10
1.6.3 Establishing a Connection with the SSH Server 10
1.6.4 Restoring an Established SSH Client Session 11
1.6.5 Disconnecting a Suspended SSH Client Session 11
1.7 Configuring SCP Client 12
1.7.1 Overview 12
1.7.2 Procedure 12
1.8 Configuring SFTP Client 13
1.8.1 Overview 13
1.8.2 Procedure 13
1.9 Monitoring 14
1.10 Configuration Examples 15
1.10.1 Configuring Line Password Authentication for SSH Users 15
1.10.2 Configuring Local User Authentication for SSH Clients 16
1.10.3 Configuring AAA Authentication for SSH Clients 18
1.10.4 Configuring Public Key Authentication for SSH Clients 20
1.10.5 Configuring SCP Server 22
1.10.6 Configuring SFTP Server 23
1.10.7 Configuring SSH Client 25
1.10.8 Configuring SCP Client 25

1.10.9 Configuring SFTP Client 26

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.

Note

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 four public key algorithms: RSA, DSA, Elliptic Curves Cryptography (ECC), and SM2 (Elliptic Curves Public Key Cryptography).

- 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.

- SM2

  Elliptic Curve Pubic Key Cryptography is a public key cryptography algorithm independently designed by China, which is a national secret algorithm based on ECC, and is used to replace the RSA algorithm in the commercial cryptography of China. The password is complex, processing speed is fast, and machine performance consumption is small.

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 SFTP Server

- 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 supports RSA and SM2 keys. SSHv2 supports DSA, RSA, and SM2 keys. If the RSA or SM2 key has been generated, both SSH1 and SSH2 are available. If only the DSA key is generated, only SSH2 is available.
- A longer public key provides higher security but slower calculation speed and higher CPU usage.

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** | **sm2** }

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** | **sm2dh_sm3** } *

Ruijie SSHv2 servers support diffie-hellman-group14-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, ecdh_sha2_nistp521 and sm2dh_sm3 for key exchange, and SSHv1 servers support none by default.

(5) (Optional) Configure the minimum length of the key generated by the key exchange algorithm of the SSH server.

ip ssh dh-exchange min-len { **1024** | **2048** }

The default minimum length is **2048** bytes.

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 { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-cbc** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **blowfish-cbc** | **cbc** | **ctr** | **des-cbc** | **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 SHA2-256, SHA2-512, and SM3 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** | **sm2** } *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 Remote Copy Protocol (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 SFTP Server

1.5.1 Overview

After the SSH File Transfer Protocol (SFTP) server function is configured on the device, users can use commands of the SFTP client console to upload files to and download files from the device. All the data exchanged in this process is transmitted in encrypted mode to provide high security.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the SFTP server function.

ip sftp server enable

The SFTP server function is disabled by default.

(4) (Optional) Configure the root path for uploading files to or downloading files from the SFTP server.

ip sftp server topdir { **flash:/***path* | **tmp:/***path* | **usb0:/***path* }

The default root path on the SFTP server is **flash:/**.

(5) (Optional) Configure the maximum number of SFTP session connections.

ip sftp server max-sessions *session-numbers*

The maximum number of SFTP session connections is 36 by default.

1.6 Configuring SSH Client

1.6.1 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.

1.6.2 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

1.6.3 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 [-**c** { 3**des** | **aes**128-**cbc** | **aes**192-**cbc** | **aes**256-**cbc** | **aes**128-**ctr** | **aes**192-**ctr** | **aes**256-**ctr** | **aes**128-**gcm** | **aes256-gcm** | **sm4-cbc** | **sm4-ctr** } | -**l** *username* | -**m** { **hmac**-**md**5-96 | **hmac**-**md**5-128 | **hmac**-**sha**1-96 | **hmac**-**sha**1-160 | **hmac**-**sha**2-256 | **hmac**-**sha**2-512 | **hmac-sm3** } | -**p** *port-num* | **-v** { **1** | **2** }] * { *ipv4-address* | *ipv6-address* | *hostname* } [/**source** { **ip** ipv4-address | **ipv**6 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, AES256-CTR, AES128-GCM, and AES256-GCM. In addition, SM4 (128-bit key) is supported: SM4-CBC and SM4. 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.

1.6.4 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*

1.6.5 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.

1.7 Configuring SCP Client

1.7.1 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.

1.7.2 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 [-**c** { 3**des** | **aes**128-**cbc** | **aes**192-**cbc** | **aes**256-**cbc** | **aes**128-**ctr** | **aes**192-**ctr** | **aes**256-**ctr** | **aes**128-**gcm** | **aes256-gcm** | **sm4-cbc** | **sm4-ctr** } | -**m** { **hmac**-**md**5-96 | **hmac**-**md**5-128 | **hmac**-**sha**1-96 | **hmac**-**sha**1-160 | **hmac**-**sha**2-256 | **hmac**-**sha**2-512 | **hmac-sm3** } | -**p** *port-num* | **-v** { **1** | **2** }] * *source-file destination-file* [/**source** { **ip** ipv4-address | **ipv**6 ipv6-address | interface interface-type interface-number }] [/vrf vrf-name]

1.8 Configuring SFTP Client

1.8.1 Overview

After the local device is configured as the SFTP client, you can connect to the SFTP server by using an SFTP command to upload and download files locally or remotely in the client console. All the data exchanged in this process is transmitted in encrypted mode to provide high security.

1.8.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the source interface used by the SFTP client.

ip sftp client source-interface interface-type interface-number

No source interface is configured for the SFTP client by default.

After the source interface is configured, the SFTP client uses the IP address of this interface as the global source address. If no source interface is configured, the device obtains the source address of the SFTP packets by querying the destination address in the corresponding route. If no source interface or address is specified separately for an SFTP connection, the global configuration applies.

(4) (Optional) Configure an SSH version for global SFTP connections.

ip sftp client version { **1** | **2** }

SSHv2 is used for global SFTP connections by default.

(5) (Optional) Configure the global SSH encryption algorithms supported by the SFTP client.

ip sftp client cipher-mode { **3des | aes128-cbc | aes128-ctr | aes128-gcm | aes192-cbc | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm** | **sm4-cbc** | **sm4-ctr** }

The SFTP client supports the following encryption algorithms by default: 3DES-CBC, AES-128-CBC, AES128-CTR, AES128-GCM, AES-192-CBC, AES192-CTR, AES-256-CBC, AES256-CTR, AES256-GCM, SM4-CBC, and SM4-CTR.

(6) (Optional) Configure the global SSH message authentication algorithms supported by the SFTP client.

ip sftp client hmac-algorithm { **hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 | hmac-sha2-256 | hmac-sha2-512 | hmac-sm3** }

SSHv1 does not support any message authentication algorithms, and SSHv2 supports the following message authentication algorithms by default: HMAC-MD5-96, HMAC-MD5-128, HMAC-SHA1-96, HMAC-SHA1-160, HMAC-SHA2-256, HMAC-SHA2-512, and HMAC-SM3.

(7) (Optional) configure the global Diffie–Hellman (DH) key exchange algorithms used by the SFTP client.

ip sftp client key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 | ecdh_sha2_nistp256 | ecdh_sha2_nistp384 | ecdh_sha2_nistp521 | **sm2dh_sm3** }

SSHv1 does not support any key exchange algorithms, and SSHv2 supports the following key exchange algorithms by default: diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1,

diffie-hellman-group1-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, ecdh_sha2_nistp521, and sm2dh_sm3.

(8) (Optional) Configure the top directory on the SFTP client.

ip sftp client topdir { *WORD* | **flash:**/*path* | **tmp:**/*path* | **usb0:**/*path* }

The default top directory on the SFTP client is **flash:/**.

(9) (Optional) Configure a rate limit for file transfer using SFTP.

ip sftp client speed-limit *speed-limit-rate*

The default rate limit for file transfer using SFTP is 8192 kbit/s.

(10) Configure the device as the SFTP client, connect it to the SFTP server, and enter the SFTP client console to manage files.

sftp [-c { 3des | aes128-cbc | aes128-ctr | aes128-gcm | aes192-cbc | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | sm4-cbc | sm4-ctr } | -k { dh_group14_sha1 | dh_group1_sha1 | dh_group_exchange_sha1 | ecdh_sha2_nistp256 | ecdh_sha2_nistp384 | ecdh_sha2_nistp521 | sm2dh_sm3 } | -m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 | hmac-sha2-256 | hmac-sha2-512 | hmac-sm3 } | -p *port-num* | -v { 1 | 2 }] * { *user@hostname* | *user@ip-address* } [/**source** { ip *ipv4-address* | **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }] [**/vrf** *vrf-name*]

1.9 Monitoring

Run the **show** command to check the configuration.

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.

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** | **sm2** }	Displays partial public key information of the SSH server.
show ssh-sessions	Displays information about established SSH client sessions.

Command	Purpose
debug ssh	Debugs sessions of the SSH server.
debug ssh client	Debugs sessions of the SSH client.

1.10 Configuration Examples

1.10.1 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 **Abc123456**.

```
Device(config)# line vty 0 4
Device(config-line)# password Abc123456
```

(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 **Abc123456**, 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 dh-exchange min-len: 2048
SSH SFTP 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$36e$17V7Zlip85+o$
!
```

1.10.2 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 **Abc123456**.

```
Device(config)# username hostname1 password Abc123456
```

(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 **Abc123456**. 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 dh-exchange min-len: 2048
SSH SFTP 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$204$ItROApnKrcmH$
!
enable service ssh-server
!
line console 0
line vty 0 4
 login local
!
```

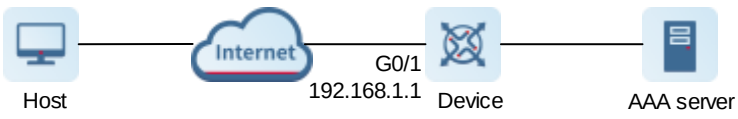
1.10.3 Configuring AAA Authentication for SSH Clients

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 **Abc123456** on the AAA server. (For details about AAA server configuration, see *Configuring AAA*.)

(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 **Abc123456**. 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 dh-exchange min-len: 2048
SSH SFTP 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
!
```

1.10.4 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 1.10.2 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$204$ItROApnKrcmH$
!
ip ssh peer hostname1 public-key rsa flash:id_rsa.pub
```

```
!
enable service ssh-server
!
line console 0
line vty 0 4
 login local
!
```

1.10.5 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 1.10.2 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$204$ItROApnKrcmH$
!
enable service ssh-server
!
ip scp server enable
!
line console 0
line vty 0 4
 login local
!
```

1.10.6 Configuring SFTP Server

1. Requirements

The device functions as the SFTP server to receive file upload and download commands from the SFTP client.

2. Topology

Figure 1-6 Topology for Configuring the SFTP Server

3. Notes

- Enable the SSH service and configure the username and password.
- Enable the SFTP server function.

4. Procedure

(1) Enable the SSH service.

```
Device> enable
Device# configure terminal
Device(config)# enable service ssh-server
Device(config)# username hostname1 password Abc123456
```

(2) Enable the SFTP server function.

```
Device(config)# ip sftp server enable
```

(3) Connect the PC to the SFTP server using the SFTP client or the **sftp** command.

```
PC> sftp ruijie@192.168.1.1
Connected to 192.168.1.1.
sftp>
```

5. Verification

Run the **ls** command to check the files in the device directory.

```
sftp> ls -l
drwxrwxrwx    2 root     root          160 Dec 17  2020 addr
drwxr-xr-x    3 root     root          224 Dec 17  2020 cmpnt
-rw-rw-rw-    1 root     root        10162 Aug  8 15:30 config.text
-rw-r--r--    1 root     root         9002 Oct 22  2021 config.text.bak
-rwxrwxrwx    1 root     root          171 Aug  8 15:30 config_vsu.dat
......
sftp>
```

Check that files are downloaded to the device directory.

```
sftp> get config.text
Fetching /data/config.text to config.text
/data/config.text                                100% 2295KB   6.4MB/s   00:00
sftp>
```

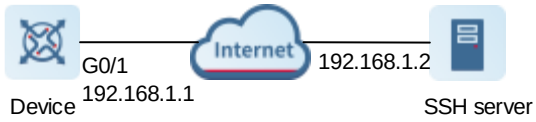
1.10.7 Configuring SSH Client

1. Requirements

When the device serves as an SSH client, the device can log in to the SSH server through SSH.

2. Topology

Figure 1-7 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 configuration.)

(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.
```

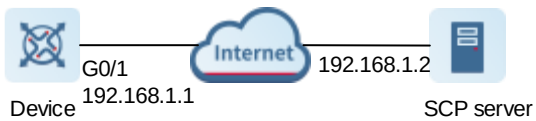
1.10.8 Configuring SCP Client

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 1-8 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 configuration.

(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# scp 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# 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.
```

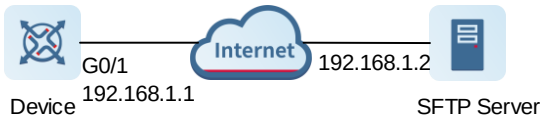
1.10.9 Configuring SFTP Client

1. Requirements

The device functions as the SFTP client. The **sftp** command can be used to establish a connection for accessing the console to upload files to and download files from the SFTP server.

2. Topology

Figure 1-9 Topology for Configuring the SFTP Client



3. Notes

- Configure users on the SFTP server.
- Run the **sftp** command to connect the device to the SFTP server and access the console.
- Run the **put** and **get** commands to upload and download files.

4. Procedure

(1) Configure available users on the SFTP server. (The configuration is omitted. For details, see the *SFTP Server User Manual*.)

(2) Run the **sftp** command on the device to access the client console.

```
Device> enable
Device# sftp admin@192.168.1.2
%Trying 192.168.1.2, 22,...open
admin@192.168.1.2's password:
Connected to 192.168.1.2:22.
sftp>
```

(3) Run the **get** command to copy the **file.txt** file from the SFTP server to the flash drive of the device.

```
sftp> get file.txt
```

(4) Run the **put** command to copy the local file **file.txt** to the SFTP server.

```
sftp> put file.txt
```

5. Verification

- Check that the file on the SFTP server is copied to the local device.

```
sftp> get file.txt
Fetching /home/admin/file.txt to file.txt
/home/admin/file.txt                                  100% 2295KB   1.7MB/s
00:00
sftp>
```

- Check that the local file is copied to the SFTP server.

```
sftp> put file.txt
Uploading file.txt to /home/admin/file.txt
file.txt                                             100% 2295KB  1.5MB/s   00:00
sftp>
```

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 and port security 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 Layer 2 Ethernet interface, Layer 2 aggregate interface, Layer 3 Ethernet interface, and Layer 3 aggregate interface as excluded ports for address binding.
- After the global IP-MAC address binding function is configured, Telnet to the port of the local device fails because packets not matching the binding rules are discarded. To prevent Telnet disconnection, you need to set the Telnet interface as an excluded port or configure a security channel rule to skip search on global IP addresses and MAC addresses and permit Telnet packets.

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 5

1.6.1 Overview 5

1.6.2 Restrictions and Guidelines 5

1.6.3 Procedure (Global Configuration Mode) 5

1.6.4 Procedure (Interface Configuration Mode) 5

1.7 Configuring Secure Address Binding 6

1.7.1 Overview 6

1.7.2 Restrictions and Guidelines 6

1.7.3 Procedure (Global Configuration Mode) 6

1.7.4 Procedure (Interface Configuration Mode) 6

1.8 Enabling Binding Log Filtering 7

1.8.1 Overview 7

1.8.2 Procedure 7

1.9 Monitoring 7

1.10 Common Errors 7

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.

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 addresses, namely, source MAC addresses, or Layer 3 addresses, namely, IP addresses or IP-MAC address bindings. 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 the port security function and other access control functions, such as IEEE 802.1X or IP Source Guard, are configured, a packet needs to meet only one security check rule to enter the port. For example, when the port security function and IEEE 802.1X are configured, and the MAC field of the packet meets the requirements of the static MAC address configured for IEEE 802.1X or the port security function, the packet can be forwarded to the port.
- If a security channel or the global IP address and MAC address binding is configured for the port, packets that meet the requirements of the security channel or global IP address and MAC address binding will bypass the security check of port and enter the port.

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 Layer 2 Ethernet interfaces and link aggregations.
- 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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. Secure Address Preemption

After this function is enabled, a static secure address can be successfully configured by forcing a dynamic secure address (not fixed) to get offline after the number of secure addresses reaches the maximum value.

4. 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 secure address preemption.

switchport port-security preempt

Secure address preemption is disabled by default.

(7) 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 (Global Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

- 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.

1.6.4 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Configure static secure addresses for ports.

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 (Global Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

- 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.

1.7.4 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Configure security bindings for a port.

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) 5
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 Layer 2 Ethernet interface or Layer 2 link aggregation. 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 a Layer 2 Ethernet interface, Layer 2 link aggregation, or member port of a Layer 2 link aggregation.

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* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *ipv4-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 IP Source Guard on a VLAN.

ip 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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* [**inner-vlan** *inner-vid*] [**vxlan** *vni*] | **vxlan** *vni* } *ipv4-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*] [**vxlan** *vni*]	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 5

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 Layer 2 Ethernet interface or Layer 2 link aggregation. 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

interface aggregateport *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 a Layer 2 Ethernet interface or link aggregation.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 a Layer 2 Ethernet interface or link aggregation.

  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 9

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 Layer 2 Ethernet Interface or link aggregation. 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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.

Command	Purpose
show savi ipv6 check source [*ipv6-address* | **interface** *interface-type interface-number*]	Displays effective IPv6 SAVI filtering entries.

1.5 Configuration Examples

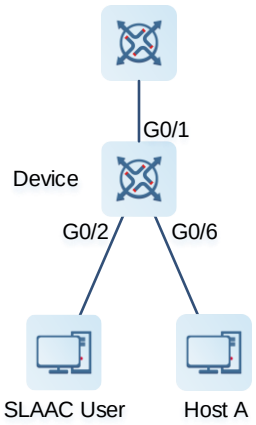
1.5.1 Configuring SAVI in an SLAAC-Only Scenario

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 0/3
Device(config-if-GigabitEthernet 0/3)# savi ipv6 check source ip-address mac-address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

```
Device# show savi ipv6 check source
Total entries found: 2
No.    Ipv6 Address                          Mac Address    VLAN Interface Filter
------ ------------------------------------- -------------- ---- --------- --
0     10::f816:3eff:fed7:cfb4                fa16.3ed7.cfb4 1    Gi0/2     IP+MAC
1     fe80::f816:3eff:fed7:cfb4              fa16.3ed7.cfb4 1    Gi0/2     IP+MAC
```

6. Configuration Files

```
!
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 0/3
 savi ipv6 check source ip-address mac-address
!
end
```

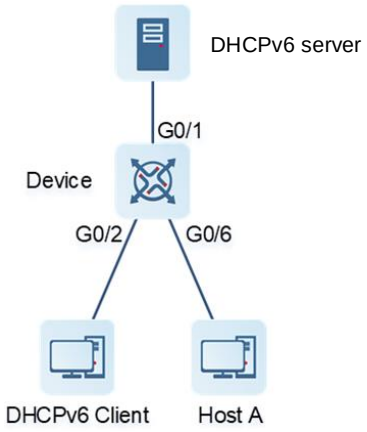
1.5.2 Configuring SAVI in a DHCPv6-Only Scenario

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 0/3
Device(config-if-GigabitEthernet 0/3)# savi ipv6 check source ip-address mac-address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

```
Device# show savi ipv6 check source
Total entries found: 2
No.    Ipv6 Address                          Mac Address    VLAN Interface Filter
------ ------------------------------------- -------------- ---- --------- ---
0      1001::1                               fa16.3e9b.0b58 1    Gi0/2     IP+MAC
```

```
1     fe80::f816:3eff:fe9b:b58              fa16.3e9b.0b58 1    Gi0/2     IP+MAC
```

6. Configuration Files

```
!
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 0/3
 savi ipv6 check source ip-address mac-address
!
end
```

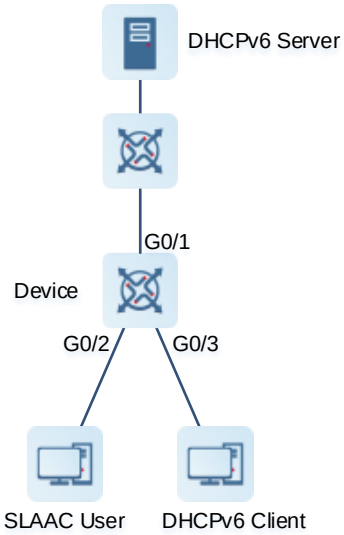
1.5.3 Configuring SAVI in an SLAAC and DHCPv6 Deployment Scenario

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 0/3
Device(config-if-GigabitEthernet 0/3)# savi ipv6 check source ip-address mac-address
```

5. Verification

Run the **show savi ipv6 check source** command to check SAVI filtering entries.

```
Device# show savi ipv6 check source
Total entries found: 4
No.    Ipv6 Address                          Mac Address    VLAN Interface Filter
------ ------------------------------------- -------------- ---- --------- ---
0     1001::1                               fa16.3e9b.0b58 1    Gi0/3     IP+MAC
1     fe80::f816:3eff:fe9b:b58              fa16.3e9b.0b58 1    Gi0/3     IP+MAC
2     1001::f816:3eff:fed7:cfb4             fa16.3ed7.cfb4 1    Gi0/2     IP+MAC
3     fe80::f816:3eff:fed7:cfb4             fa16.3ed7.cfb4 1    Gi0/2     IP+MAC
```

6. Configuration Files

```
!
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 0/3
 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 a Layer 2 Ethernet interface or link aggregation 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 a Layer 2 Ethernet interface or link aggregation.

- 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *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 Configuring Dynamic ARP 3

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.

⚠ Caution

- 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(5) Configure interfaces as DAI trusted interfaces.

ip arp inspection trust

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 interfaces.

1.4 Configuration Examples

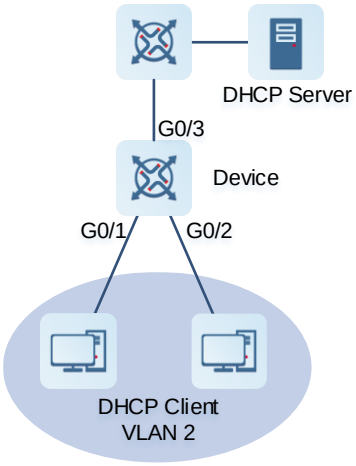
1.4.1 Configuring Dynamic ARP

1. Requirements

Hosts can use only addresses assigned by a legitimate DHCP server to prevent ARP spoofing.

2. Topology

Figure 1-1 Configuring DAI



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.

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
```

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
```

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
```

7. Common Errors

An interface configured with security limitations is set as a DAI trusted interface.

Contents

1 Configuring ARP Spoofing Prevention 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 ARP Spoofing Prevention 2

1.3 Monitoring 2

1.4 Configuration Examples 2

1.4.1 Configuring ARP Spoofing Prevention 2

1 Configuring 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 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.

- 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 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. ARP Spoofing Prevention

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 ARP Spoofing Prevention

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

(4) Enable ARP spoofing prevention.

anti-arp-spoofing ip *ipv4-address*

ARP spoofing prevention is disabled by default.

ARP spoofing prevention is supported only on Layer 2 Ethernet interfaces or link aggregations.

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 ARP spoofing prevention.

1.4 Configuration Examples

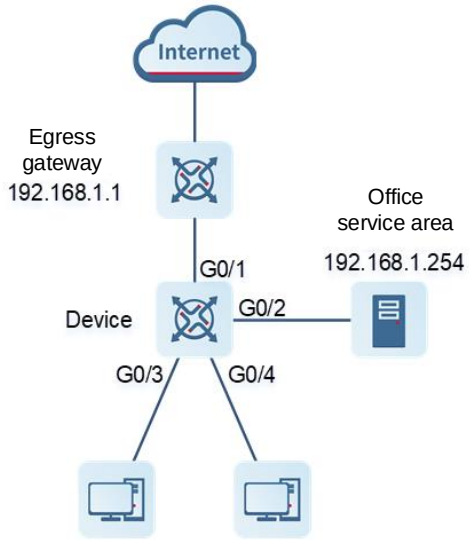
1.4.1 Configuring ARP Spoofing Prevention

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.

2. Topology

Figure 1-1 Configuring ARP Spoofing Prevention



3. Notes

Enable ARP spoofing prevention on the access interface.

4. Procedure

Configure 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
```

5. Verification

Run the **show anti-arp-spoofing** command to check for data on 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
```

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 Overview....1
1.1.2 Basic Concepts....1
1.1.3 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 Monitoring....6
1.6 Configuration Examples....7
1.6.1 Configuring Basic Functions of CPP....7

1 Configuring CPP

1.1 Introduction

1.1.1 Overview

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.

1.1.2 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.

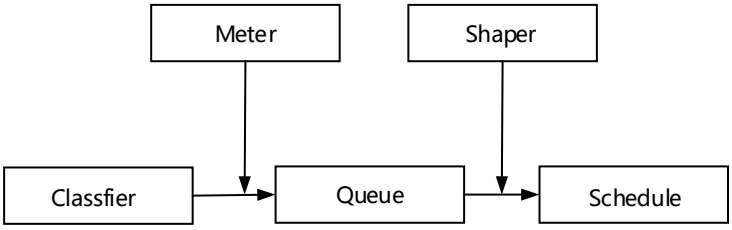
5. CPU Interface

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.

1.1.3 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.

Note

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.

Note

Only the SP scheduling policy is supported and cannot be modified.

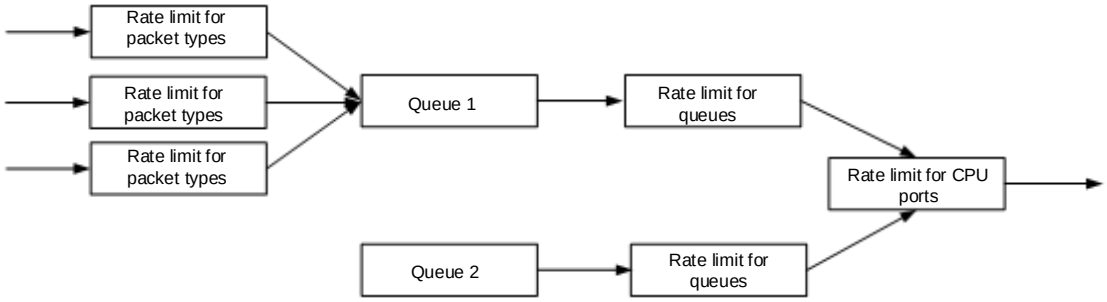
5. Shaper

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

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 NFPP*.
- 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.

- 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.

- Configure a bandwidth for a priority queue.

  cpu-protect traffic-class *traffic-class-number* **bandwidth** *bandwidth-value*

  The default bandwidth values of queues 1–6 are 1500 pps, and the default bandwidth value of queue 7 is 2000 pps.

  No bandwidth is configured for a priority queue by default.

- Configure a bandwidth for the CPU interface.

  cpu-protect cpu bandwidth *bandwidth-value*

  The default bandwidth for a CPU port is 4500 pps.

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 **600** seconds.

(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 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 enabled 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 **clear** commands to clear 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
clear cpu-protect counters [**device** *device-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*]	Displays the configuration and statistics of a packet type.
show cpu-protect traffic-class *traffic-class-number* [**device** *device-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*]	Displays all the configuration and statistics of CPP.
show cpu-protect statistics [**interface** *interface-type interface-number*]	Displays the statistics on a CPP port.

Command	Purpose
show cpu-protect statistics type *packet-type*	Displays the statistics of a packet type on a CPP port.
show cpu-protect hardware-statistics [**device** *device-number*]	Displays the hardware statistics of a CPP packet type.
show cpu-protect linkage summary	Displays the protocol correlation state.

1.6 Configuration Examples

1.6.1 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 priority queues 0 to 6 is 750 pps, the bandwidth for priority queue 7 is 1000 pps, and the bandwidth for the CPU interface is 2250 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 500
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 500
DeviceA(config)# end
```

4. Verification

Run the **show cpu-protect** command to view the configuration and statistics.

```
DeviceA# show cpu-protect
```

```
%cpu port bandwidth: 2250(pps)
Traffic-class   Bandwidth(pps)  Rate(pps)  Drop(pps)
-------------   --------------  ---------  ---------
 0            750           0        0
 1            750           0        0
 2            750           0        0
 3            500           0        0
 4            750           0        0
 5            750           0        0
 6            750           0        0
 7            1000          0        0
Packet Type           Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total
Total Drop    DropTime
----------------------  -------------  --------------  ---------  ---------
---------    ----------    ----------------------------
arp                  1            500           0        0        0           0
arp-auth-proxy         2            256           0        0        0           0
arp-sdn               1            50            0        0        0           0
bfd                  6            500           0        0        0           0
bgp                  4            128           0        0        0           0
bgpv6                4            128           0        0        0           0
bpdu                 6            64            0        0        0           0
cdp                  5            128           0        0        0           0
cfm                  5            64            0        0        0           0
dhcp-relay-c          2            256           0        0        0           0
dhcp-relay-s          2            256           0        0        0           0
dhcp-sdn             2            512           0        0        0           0
dhcp6-client          2            256           0        0        0           0
dhcp6-relay           2            256           0        0        0           0
dhcp6-server          2            256           0        0        0           0
dhcps                2            256           0        0        0           0
dhcps6               2            256           0        0        0           0
dldp                 6            200           0        0        0           0
dldpv6               6            200           0        0        0           0
dns-client            3            220           0        0        0           0
dns-server            3            220           0        0        0           0
dot1x                2            256           0        0        0           0
dvmrp                4            64            0        0        0           0
```

efm	5	64	0	0	0	0
erps	5	64	0	0	0	0
fcoe-fip	4	256	0	0	0	0
fcoe-local	4	256	0	0	0	0
fpga-cfg	7	1000	0	0	0	0
fpga-notify	0	500	0	0	0	0
gvrp	5	64	0	0	0	0
hop-limit	0	256	0	0	0	0
icmp	3	400	0	0	0	0
icmpv6-echo	3	800	0	0	0	0
igmp	2	256	0	0	0	0
igmp-drop	2	500	0	0	0	0
ip-option	0	200	0	0	0	0
ip-option6	0	200	0	0	0	0
ipv6-all	0	100	0	0	0	0
isis	4	256	0	0	0	0
l3mtu-fail	0	100	0	0	0	0
lacp	5	128	0	0	0	0
lldp	5	128	0	0	0	0
local-ipv4	3	550	0	0	0	0
local-ipv6	3	400	0	0	0	0
mac-move	0	64	0	0	0	0
madp	6	150	0	0	0	0
mlagv4	5	1024	0	0	0	0
mlagv6	5	1024	0	0	0	0
mld	2	256	0	0	0	0
mld-drop	2	64	0	0	0	0
nacm-drop	2	64	0	0	0	0
nd-non-snp	1	256	0	0	0	0
nd-snp-na-sdn	1	100	0	0	0	0
nd-snp-ns-na	1	256	0	0	0	0
nd-snp-ns-na-l3	1	10000	0	0	0	0
nd-snp-ra-redirect	1	64	0	0	0	0
nd-snp-ra-redirect-l3	1	1500	0	0	0	0
nd-snp-rs	1	64	0	0	0	0
nd-snp-rs-l3	1	1500	0	0	0	0
ndsnp	1	512	0	0	0	0

ntp	3	1000	0	0	0	0
ntpv6	3	1000	0	0	0	0
option82	2	256	0	0	0	0
ospf	5	512	0	0	0	0
ospf3	4	512	0	0	0	0
other	0	256	0	0	0	0
pim	4	64	0	0	0	0
pimv6	4	64	0	0	0	0
pvst	6	300	0	0	0	0
rerp	5	64	0	0	0	0
reup	5	64	0	0	0	0
rip	4	64	0	0	0	0
ripng	4	64	0	0	0	0
rldp	5	64	0	0	0	0
rt-host	4	128	0	0	0	0
rt-hostv6	4	128	0	0	0	0
sdn	0	256	0	0	0	0
sflow	0	512	0	0	0	0
snmp	3	550	0	0	0	0
snp-mac-learning	0	10	0	0	0	0
ssh	3	550	0	0	0	0
stargv-ipmc	2	64	0	0	0	0
stargv6-ipmc	1	64	0	0	0	0
tcp-syn	3	1000	0	0	0	0
telnet	3	550	0	0	0	0
tpp	6	64	0	0	0	0
trill	4	500	0	0	0	0
trill-isis	4	256	0	0	0	0
trill-local	4	256	0	0	0	0
trill-oam	4	64	0	0	0	0
ttl-hop-limit	0	512	0	0	0	0
ttl0	0	64	0	0	0	0
ttl1	0	256	0	0	0	0
tunnel-bpdu	2	64	0	0	0	0
tunnel-gvrp	2	64	0	0	0	0
udp-flood	3	0	0	0	0	0
unknown-v4mc	1	64	0	0	0	0

```
unknown-v6mc          1          64          0          0          0          0
v4uc-route            3          200         0          0          0          0
v6uc-route            1          100         0          0          0          0
vrrp                  6          64          0          0          0          0
vrrpv6                6          64          0          0          0          0
web-auth              2          400         0          0          0          0
xgv-ipmc              2          64          0          0          0          0
xgv6-ipmc             1          64          0          0          0          0
```

5. Configuration Files

Device A configuration file

```
!
cpu-protect type arp bandwidth 500
cpu-protect type arp traffic-class 1
cpu-protect type ospf traffic-class 5
cpu-protect type v4uc-route traffic-class 3
cpu-protect traffic-class 3 bandwidth 500
!
```

Contents

1 Configuring NFPP 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Rate Limiting Threshold and Attack Identification for Hosts 3
1.1.4 Rate Limiting and Attack Identification for Ports 4
1.1.5 Hardware Isolation 4
1.1.6 Monitoring Time 4
1.1.7 Trust Host 4
1.2 Configuration Task Summary 4
1.3 Configuring ARP Guard 5
1.3.1 Overview 5
1.3.2 Restrictions and Guidelines 5
1.3.3 Procedure (Global Configuration) 6
1.3.4 Procedure (Interface Configuration) 8
1.4 Configuring IP Guard 8
1.4.1 Overview 8
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure (Global Configuration) 10
1.4.4 Procedure (Interface Configuration) 11
1.5 Configuring TCP-SYN Guard 11
1.5.1 Overview 11

1.5.2 Restrictions and Guidelines 12
1.5.3 Procedure (Global Configuration) 12
1.5.4 Procedure (Interface Configuration) 13
1.6 Configuring ICMP Guard 14
1.6.1 Overview 14
1.6.2 Restrictions and Guidelines 14
1.6.3 Procedure (Global Configuration) 15
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

1.1.1 Overview

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.

1.1.2 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. ARP Source Suppression

When IP packets are sent to an unconfigured destination IP address at a high rate, they are forwarded to the CPU, triggering the device to send 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, isolate the source of the attack and enable the function of ARP source suppression. If IP packets that trigger ARP requests exceed the threshold in the specified period, the IP packets out of the threshold are discarded.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

1.1.3 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.

Note

- 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.

1.1.4 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.

1.1.5 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.

Note

Only ARP guard can be configured with the global isolation and forwarding function and the rate limit function for port-based isolation and forwarding.

1.1.6 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.

1.1.7 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.
- Suppress the ARP source. In this type of attacks, ARP requests are triggered through IP packets to consume CPU resources. If the number of IP packets with inexistent destination IP address exceeds the threshold in the specified period, the IP packets out of the threshold are discarded.
- 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.
- ARP source suppression conflicts with the isolation function of IP guard scan. If the latter is enabled, you cannot enable the function of ARP source suppression.
- 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 rate limiting threshold for each source IP address, each source MAC address, and each interface is 30, 30, and 256, in pps.

(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 attack threshold for each source IP address, each source MAC address, and each interface is 200, 200, and 400, in pps.

(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, in packets per 10 seconds.

(13) Enable the function of ARP source suppression.

arp-guard suppress-mode enable

The function of ARP source suppression is disabled by default.

(14) Configure a threshold of ARP source suppression.

arp-guard suppress-threshold *suppress-threshold*

The default threshold of ARP source suppression is **5** pps.

(15) Configure the period of ARP source suppression.

arp-guard suppress-period *interval*

No period of ARP source suppression is configured by default.

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.
- The isolation function of IP guard conflicts with the function of ARP source suppression. Therefore, you cannot configure the two functions at the same time.
  - If you enable them at the same time, you cannot configure the isolation time of IP guard.
  - If you enable the function of ARP source suppression and configure the global or local isolation time for IP guard, you cannot enable the IP guard function.

  To configure the isolation function of IP guard, make sure to disable the function of ARP source suppression.
- 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) Configure the monitoring time of IP guard.

ip-guard monitor-period *interval*

The default monitoring time of IP guard is **600** seconds.

(6) 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.

(7) (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 rate limiting threshold for each source IP address and each interface is 20 and 100, in pps.

(8) Configure a global attack threshold of IP guard.

ip-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

By default, the attack threshold for each source IP address and each interface is 200 and 400, in pps.

(9) 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, in packets per 10 seconds.

(10) (Optional) Configure the trusted hosts of IP guard.

ip-guard trusted-host { *ipv4-address mask* | *ipv6-address/prefix-length* }

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 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.

(6) 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

By default, the global TCP-SYN guard function is enabled.

(5) 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.

(6) 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.

(7) 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 rate limiting threshold for each source IP address and each interface is 20 and 100, in pps.

(8) 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 attack threshold for each source IP address and each interface is 200 and 400, in pps.

(9) (Optional) Configure the trusted hosts of TCP-SYN guard.

tcp-syn-guard trusted-host { *ipv4-address mask* | *ipv6-address/prefix-length* }

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 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) Configure the monitoring time of ICMP guard.

icmp-guard monitor-period *interval*

The default monitoring time of ICMP guard is **600** seconds.

(6) Configure the maximum number of monitored hosts.

icmp-guard monitored-host-limit *number*

The maximum number of monitored hosts is **20000** by default.

(7) 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 rate limiting threshold for each source IP address and each interface is 400 and 500, in pps.

(8) Configure the global attack threshold of ICMP guard.

icmp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

By default, the attack threshold for each source IP address and each interface is 600 and 800, in pps.

(9) (Optional) Configure the trusted hosts of ICMP guard.

icmp-guard trusted-host { *ipv4-address mask* | *ipv6-address/prefix-length* }

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 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) Configure the monitoring time of DHCP guard.

dhcp-guard monitor-period *interval*

The default monitoring time of DHCP guard is **600** seconds.

(6) 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.

(7) 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 rate limiting threshold for each source MAC address and each interface is 5 and 300, in pps.

(8) Configure the global attack threshold of DHCP guard.

dhcp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

By default, the attack threshold for each source MAC address and each interface is 10 and 512, in pps.

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 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 rate limiting threshold for each source MAC address and each interface is 5 and 300, in pps.

(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 attack threshold for each source MAC address and each interface is 10 and 512, in pps.

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 rate limiting threshold for neighbor requests and advertisements, route requests, route advertisements and redirection packets, and NDSNP packets is 100, 50, 50, and 200, in pps.

(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 attack threshold for neighbor requests and advertisements, route requests, route advertisements and redirection packets, and NDSNP packets is 200, 100, 100, and 400, in pps.

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) Enter the NFPP configuration mode.

nfpp

(4) Disable all the basic types of global guard of NFPP.

no 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.

⚠ Caution

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.

Command	Purpose
clear nfpp icmp-guard hosts	Clears the monitored hosts of ICMP guard.
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 NFPP log buffer.
show nfpp arp-guard summary	Displays ARP guard configuration.
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 IP guard configuration.
show nfpp ip-guard hosts	Displays the monitored hosts of IP guard.
show nfpp ip-guard trusted-host	Displays the trusted hosts 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 trusted hosts 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 DHCPv6 guard configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored hosts of DHCPv6 guard.
show nfpp nd-guard summary	Displays the ND guard configuration.
show nfpp nd-guard hosts	Displays the trusted hosts of ND guard.
show nfpp define summary [*name*]	Displays the customized guard configuration.
show nfpp define hosts *name*	Displays the monitored hosts of the customized guard.
show nfpp define trusted-host *name*	Displays the trusted hosts of the customized guard.
show nfpp log summary	Displays the statistics of the NFPP log buffer.
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 rate limiting threshold and attack threshold.
- Configure the rate limiting threshold and attack threshold.
- Configure the rate limiting threshold and attack threshold.
- Configure the rate limiting threshold and attack threshold.
- Configure the rate limiting threshold and attack threshold of DHCPv6 guard.
- Configure the rate limiting threshold and attack threshold 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 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 trusted-host 192.168.201.46 255.255.255.255
```

Configure DHCP guard on Device A.

```
DeviceA(config-nfpp)# dhcp-guard rate-limit per-port 20
DeviceA(config-nfpp)# dhcp-guard attack-threshold per-port 30
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-port 20
DeviceA(config-nfpp)# dhcpv6-guard attack-threshold per-port 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    Enable  180          30/5/128       100/10/200      100

Maximum count of monitored hosts: 20000
Monitor period: 600s
Suppress-mode: disable
Suppress-threshold: 5pps
Suppress-period: 5s
```

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)
```

Note

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)
```

Note

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.

```
DeviceA# show nfpp tcp-syn-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 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)
```

Note

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)
```

Note

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)
```

Note

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)
```

Note

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....2
1.3 Monitoring....2
1.4 Configuration Examples....2
1.4.1 Configuring Storm Control....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.

Note

When the storm suppression threshold is set to the percentage-based bandwidth, products may convert the configured value to a multiple of the step supported by the product. 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.

Note

When the storm suppression threshold is set to kilobits-per-second, products may convert the configured value to a multiple of the step supported by the product. Therefore, the actual effective suppression threshold on a port may be smaller than the configured suppression threshold.

4. Storm Control Actions

Storm control actions are implemented when the data flow rate on a device interface surpasses the configured storm control threshold, prompting actions on that specific interface.

After storm control actions are configured, the system performs periodic checks at an interval of one storm control detection interval (10 seconds by default, configurable). If the average rate of broadcast, multicast, or unknown unicast packets received on an interface exceeds the specified threshold, the interface processes the packets received based on the configured action.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *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

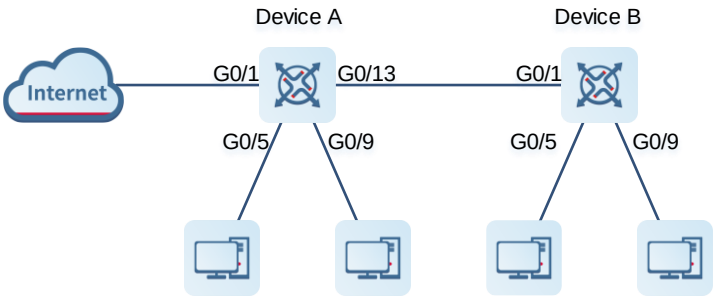
1.4.1 Configuring Storm Control

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 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 5
1.7 Configuring the Function of Denying ICMP Flood Packets 5
1.7.1 Overview 5
1.7.2 Restrictions and Guidelines 5
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....6
1.9 Configuring Attack Packet Statistics....6
1.9.1 Overview....6
1.9.2 Restrictions and Guidelines....6
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 Null Scan Attacks
- 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 Null Scan Attacks

1.6.1 Overview

After the function of denying null scan attacks is enabled, the device will proactively discard TCP packets without any flag to filter out invalid TCP packets before attack packets enter the network and protect internal servers from external attacks.

1.6.2 Restrictions and Guidelines

Typically, this function is configured on devices connected to the server.

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 null scan attacks.

ip deny null-scan

The function of denying null scan attacks is disabled by default.

1.7 Configuring the Function of Denying ICMP Flood Packets

1.7.1 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.

1.7.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.
- After this function is enabled, only the rate of bypassing ICMP packets is limited, and ICMP 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 ICMP flood packets.

ip defense icmp-flood *rate-limit*

The function of denying ICMP flood packets is disabled by default.

1.8 Configuring the Function of Denying SYN Flood Packets

1.8.1 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.

1.8.2 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.

1.8.3 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.

1.9 Configuring Attack Packet Statistics

1.9.1 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.

1.9.2 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.

1.9.3 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.

1.10 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 lose vital information and thus interrupt services.

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.
show ip deny null-scan	Displays the status of the function of denying null scan attacks.
clear ddos icmp-flood counter	Clears ICMP flood packet statistics.
clear ddos null-scan counter	Clears null scan packet statistics.
clear ddos syn-flood counter	Clears TCP SYN flood packet statistics.

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.

Note

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) Enabling the Function of Sending Security Logs to the Syslog Server

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**.

1.4.6 Enabling the Function of Sending Security Logs to the Syslog Server

1. Overview

After the function of sending security logs to the syslog server is enabled, a syslog is generated for each security log.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of sending security logs to the syslog server.

security-log send-syslog

The function of sending security logs to the syslog server is enabled by default.

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.

⚠ Caution

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.

Command	Purpose
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.
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: 1000
Store days: 300
```

```
Auto vacuum time: 05:05:00
Security-log send to syslog: enable
```

6. Configuration Files

```
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. Configuring REUP
2. Configuring RLDP
3. Configuring DLDP
4. Configuring VRRP
5. Configuring VRRP Plus
6. Configuring BFD
7. Configuring Track
8. Configuring IP Event Dampening
9. Configuring HAM
10. Configuring SYSHA

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 13
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.

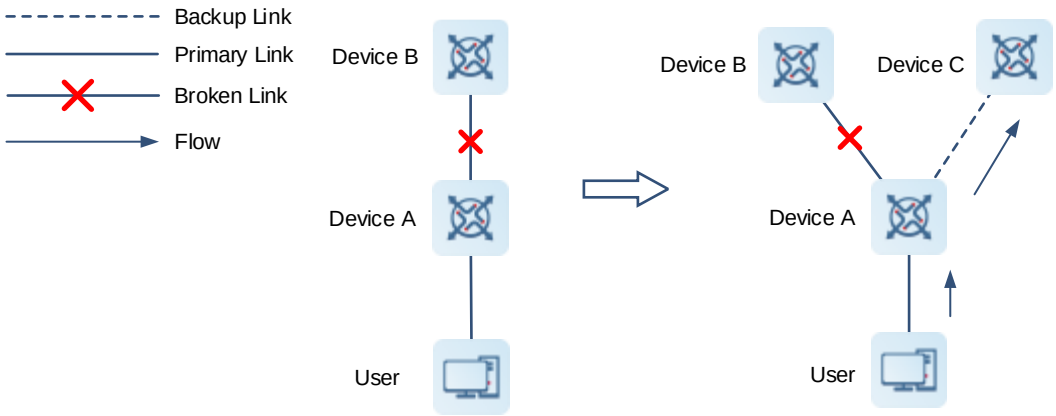
1.1 Introduction

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 Device A and distribution Device B fails, the link between the user and Device 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

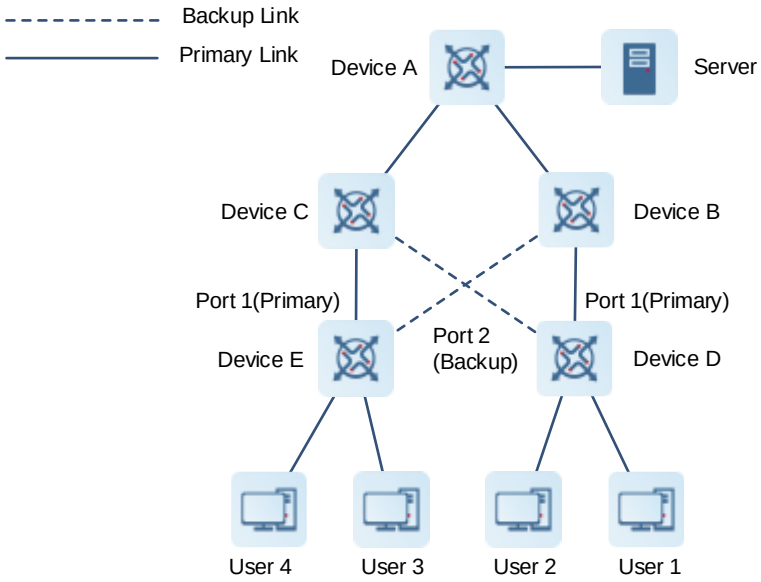
The uplink and downlink ports of a device can be added to a group at the same time, which is called a link state tracking group. If all uplink ports in the group are down, all downlink ports in this group are forced down.

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.

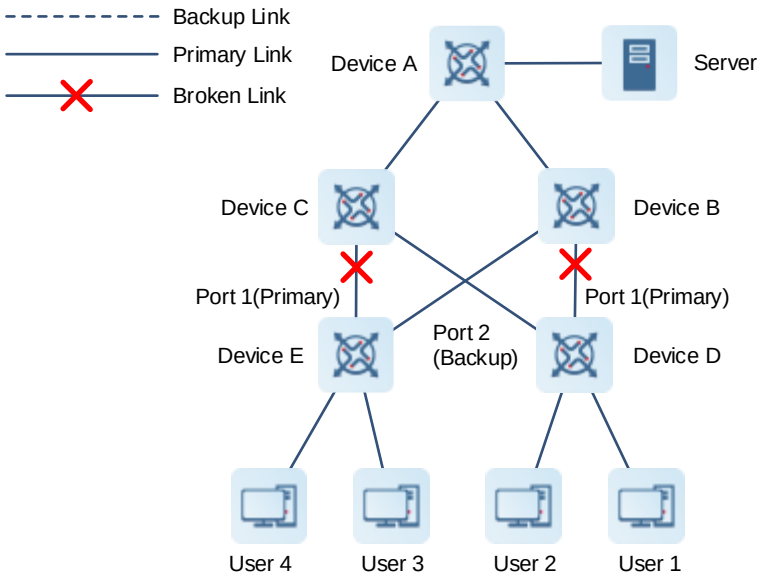
- You can specify a port as the backup port of another port to configure an REUP pair. When the two ports are normal, one link is in the forwarding state (forwarding data packets) and the other link is in the backup state (not forwarding data packets).
- When the active link is faulty, the link in the 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 Device D (Device E) are connected to uplink switches B and C (Devices 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 Device D and Device 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 Device D (Device E) have the REUP dual-link backup enabled. Port 1 works as the active port. During normal communication, Device A learns the MAC addresses of users 1 and 2 (users 3 and 4) from the port connecting to Device B (Device C).
- When port 1 of Device D (Device E) fails, port 2 quickly changes to the forwarding state and starts to forward data packets. In this case, Device A has not learned the MAC addresses of users 1 and 2 (users 3 and 4) from the port connecting to Device B (Device C). The data packets sent by the server to users 1 and 2 (users 3 and 4) are forwarded to Device C (B) by Device 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 Device D (Device E). When port 2 starts to forward packets, Device D (Device E) sends a MAC address update message to port 2.
- After receiving the MAC address update message from port 2, Device A updates the MAC address entries on the port of Device A. In this way, Device A forwards the packets sent by the server to the users, to the port connecting to Device C (Device 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, Device D (Device E) sends MAC address update packets for users 1 and user 2 (users 3 and 4) upstream when port 2 DeviceEs to the forwarding state. In this way, Device A updates the MAC addresses of users 1 and 2 (users 3 and 4) to the corresponding port and the downstream data transmission of Device 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.

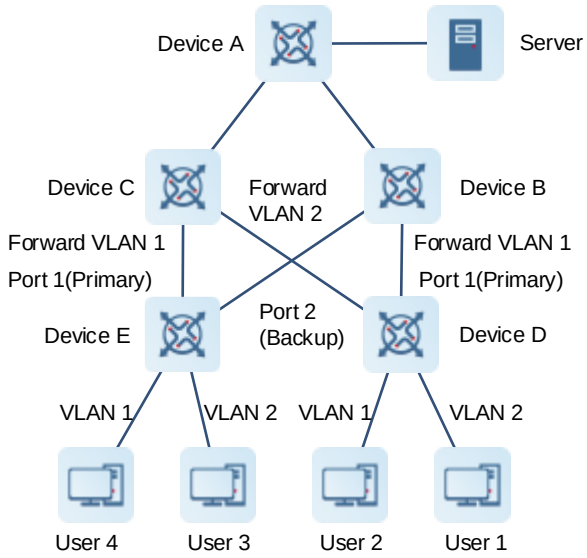
1.1.5 VLAN Load Balancing

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 Device 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 Device 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 VLAN load balancing topology



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*.
- 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 Device B is faulty, link state tracking rapidly shuts down the downstream port of Device B so that the upstream transmission of Device D is switched to Device C.

Figure 1-5 Topology with the Active Uplink Faulty

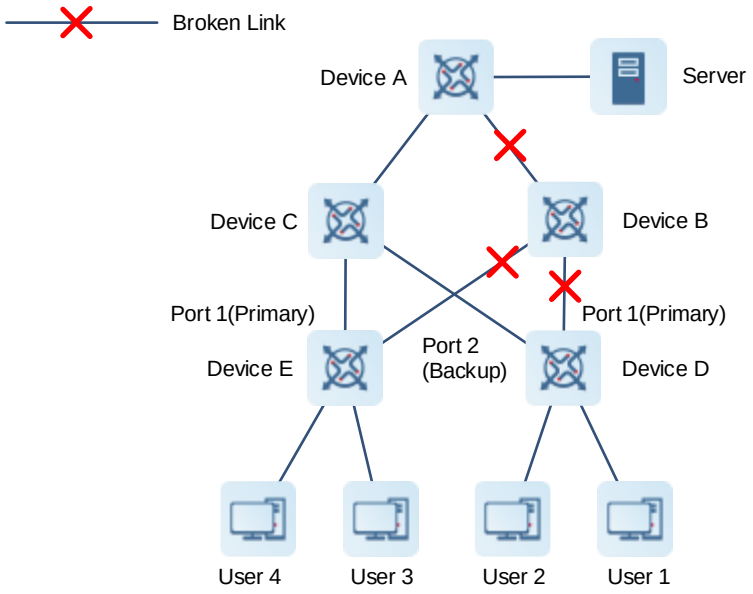


Table 1-2 Description of Link State Tracking Configuration Items

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 Layer 2 physical ports and link aggregations, but does not support member ports of a link aggregation .
- 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 Layer 3 interfaces or added to a link aggregation.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the Layer 2 Ethernet 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

- You can configure the preemption mode to determine the link to use. 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.
- 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. If the preemption mode is set to bandwidth mode, a link with a greater bandwidth is used. The value of the bandwidth attribute of a link aggregation is the actual bandwidth of the link aggregation, equal to the number of link up member ports of the link aggregation multiplied by the speed attribute value of a 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.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *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.
- 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. To update the MAC address table of the uplink switch, enable the function of sending MAC address update messages on the device where link switching occurs, and enable the function of receiving MAC address update messages on the uplink device. During link switching, if the function of sending MAC address update messages is enabled, 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. For a VLAN in which the function of processing MAC address update messages is disabled, the device can still recover the downlink transmission of uplink devices based on the MAC address update packets; however, the convergence performance will be degraded in the case of link

faults.

- Massive flooding caused by MAC address update may affect normal data transmission of the switch. Flooding packets can be reduced by configuring MAC address update groups to quickly recover data transmission. Transmission of downstream data can be rapidly recovered only after all ports in a switching path are added to the same MAC address update group.

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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *interface-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *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. You can modify the mappings between instances and VLANs by using the instance mapping function of MSTP. 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.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *interface-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode.

  interface aggregateport *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.

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 10 upstream ports and 256 downstream ports.
- 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.

1.7.3 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* [**up-delay** *interval*]]

All the link state tracking groups are disabled by default.

(4) Enter the Layer 2 Ethernet interface configuration mode.

interface *interface-type interface-number*

(5) 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.

(6) 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

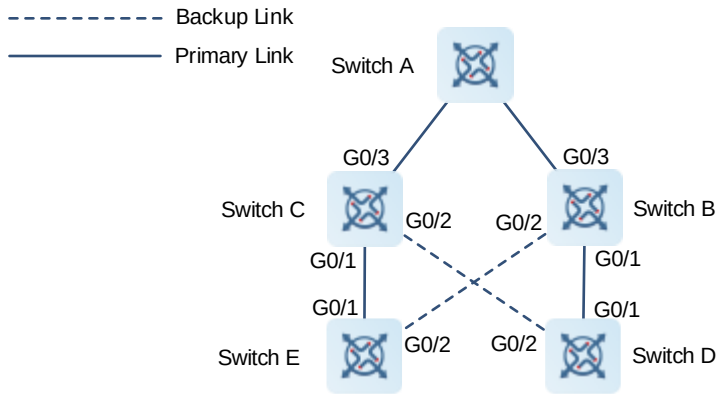
1. Requirements

To improve network reliability and ensure continuity of services between the access device and the core device, two links are deployed between core device A and each of the access devices D and E, as shown in Figure 1-6. REUP dual-link backup must be configured on the access devices. When the two links are normal, one is in the

active state and forwards packets while the other is in the standby state. When the active link becomes faulty, the link in standby state is quickly switched to the active state and starts to forward data.

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 Device D (Device E).

4. Procedure

Perform the following configuration on Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# interface gigabitethernet 0/1
DeviceD(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceD(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2
DeviceD(config-if-GigabitEthernet 0/1)# exit
```

Perform the following configuration on Device E.

```
DeviceE> enable
DeviceE# configure terminal
DeviceE(config)# interface gigabitethernet 0/1
DeviceE(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceE(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2
DeviceD(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 Device D.

```
DeviceD#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 Device E.

```
DeviceE#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

- Device D configuration file

```
hostname DeviceD
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport backup interface GigabitEthernet 0/2
!

end
```

- Device E configuration file

```
hostname DeviceE
!
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 a Layer 2 physical port or link aggregation.

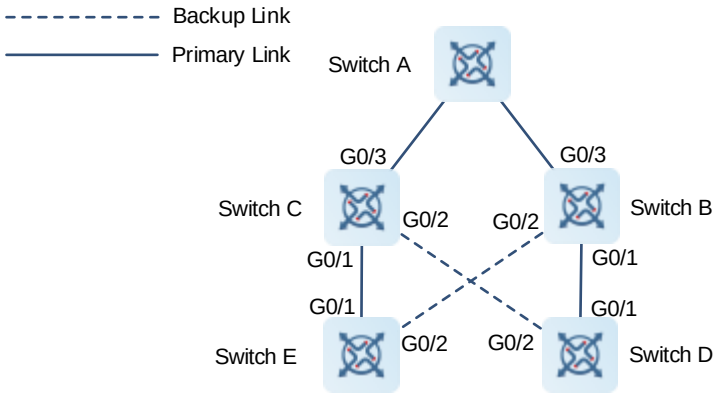
1.9.2 Configuring the MAC Address Update Function

1. Requirements

To improve network reliability and ensure continuity of services between the access device and the core device, two links are deployed between core device A and each of the access devices D and E, as shown in Figure 1-7. To accelerate packet convergence during link switch, the MAC address update function must be configured on the device.

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 Device D (Device E).
- Enable the function of receiving MAC address update packets on Device B (Device C).
- Add all ports in the REUP switching path to the same MAC address update group.
- GigabitEthernet 0/1 and GigabitEthernet 0/3 of Device B are the ports in the uplink switching path of Device D, and GigabitEthernet 0/3 and GigabitEthernet 0/2 are the ports in the uplink switching path of Device E. You can add ports GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 to the same address update group. Similarly, you can perform the configuration on Device C.
- Enable the function of receiving MAC address update packets on Device A.
- Add all ports in the REUP switching path of Device A to the same MAC address update group.

4. Procedure

Perform the following configuration on Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# mac-address-table move update transit
```

Perform the following configuration on Device E.

```
DeviceE> enable
DeviceE# configure terminal
DeviceE((config)# mac-address-table move update transit
```

Perform the following configuration on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# mac-address-table move update receive
DeviceB(config)# interface range gigabitethernet 0/1-3
DeviceB(config-if-range)# switchport mode trunk
DeviceB(config-if-range)# mac-address-table update group 1
```

Perform the following configuration on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# mac-address-table move update receive
DeviceC(config)# interface range gigabitethernet 0/1-3
DeviceC(config-if-range)# switchport mode trunk
DeviceC(config-if-range)# mac-address-table update group 1
```

Perform the following configuration on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mac-address-table move update receive
DeviceA(config)# interface range gigabitethernet 0/1-2
DeviceA(config-if-range)# switchport mode trunk
DeviceA(config-if-range)# mac-address-table update group 1
```

5. Verification

Display the configurations of the MAC address update group on device B.

```
DeviceB# 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
```

Display the configurations of the MAC address update group on device C.

```
DeviceC# 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
```

Display the configurations of the MAC address update group on device A.

```
DeviceA# 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

- Device A configuration file

```
hostname DeviceA
!
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
```

- Device B configuration file

```
hostname DeviceB
!
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
```

- Device C configuration file

```
hostname DeviceC
!
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
```

- Device D configuration file

```
hostname DeviceD
!
mac-address-table move update transit

end
```

- Device E configuration file

```
hostname DeviceE
!
mac-address-table move update transit

end
```

7. Common Errors

- A configured port is not a Layer 2 physical port or link aggregation.

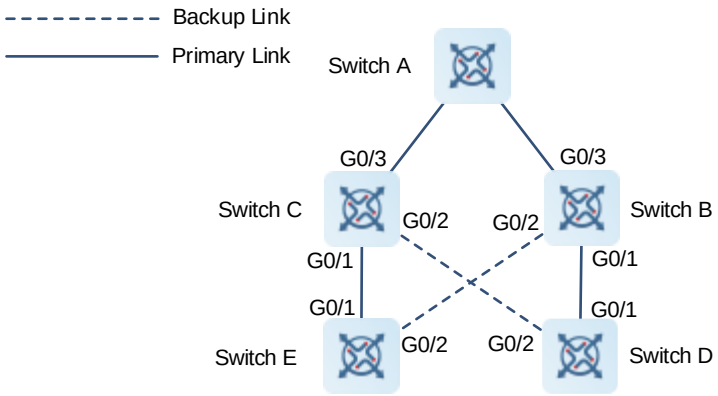
1.9.3 Configuring VLAN Load Balancing

1. Requirements

To improve network reliability and ensure continuity of services between the access device and the core device, two links are deployed between core device A and each of the access devices D and E, as shown in Figure 1-8. To make full use of the link bandwidth, the VLAN load balancing function must be enabled.

2. Topology

Figure 1-8 Topology for Configuring VLAN Load Balancing



3. Notes

- Configure instance mappings on Device D (Device 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 Device D (Device E).

4. Procedure

Perform the following configuration on Device D.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# interface gigabitethernet 0/1
DeviceD(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceD(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 prefer instance 2
DeviceD(config-if-GigabitEthernet 0/1)# exit
```

Perform the following configuration on Device E.

```
DeviceE> enable
DeviceE# configure terminal
DeviceE(config)# interface gigabitethernet 0/1
DeviceE(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceD(config-if-GigabitEthernet 0/1)# switchport backup interface gigabitethernet
0/2 prefer instance 4
DeviceD(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 Device D.

```
DeviceD# 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)
```

Run the **show interfaces switchport backup detail** command to check the dual-link backup information configured on Device E

```
DeviceE# 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

- Device D configuration file

```
hostname DeviceD
!
interface GigabitEthernet 0/1
 switchport mode trunk
 switchport backup interface gigabitethernet 0/2 prefer instance 2
!

end
```

- Device E configuration file

```
hostname DeviceE
```

```
!
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.

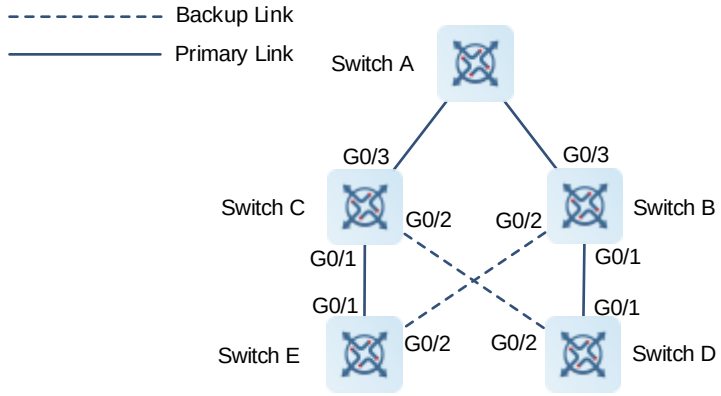
1.9.4 Configuring Link State Tracking

1. Requirements

To improve network reliability and ensure continuity of services between the access device and the core device, two links are deployed between core device A and each of the access devices D and E, as shown in Figure 1-9To forcibly switch downlink transmission upon uplink faults and ensure normal transmission of service packets, the link tracking function must be enabled on devices B and C.

2. Topology

Figure 1-9 Topology for Configuring Link State Tracking



3. Notes

- Create link state tracking group 1 on Device B (Device C).
- On Device B (Device 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 Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# link state track 1
DeviceB(config)# interface GigabitEthernet 0/1
```

```
DeviceB(config-if-GigabitEthernet 0/1)# link state group 1 downstream
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface GigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# link state group 1 downstream
DeviceB(config-if-GigabitEthernet 0/2)# exit
DeviceB(config)# interface GigabitEthernet 0/3
DeviceB(config-if-GigabitEthernet 0/3)# link state group 1 upstream
```

Perform the following configuration on Device C.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)# link state track 1
DeviceC(config)# interface GigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# link state group 1 downstream
DeviceC(config-if-GigabitEthernet 0/1)# exit
DeviceC(config)# interface GigabitEthernet 0/2
DeviceC(config-if-GigabitEthernet 0/2)# link state group 1 downstream
DeviceC(config-if-GigabitEthernet 0/2)# exit
DeviceC(config)# interface GigabitEthernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# link state group 1 upstream
```

5. Verification

Run the **show link state group** command to check whether the link tracking group is created on Device B.

```
DeviceB# show link state group
Link State Group:1  Status: enabled, Down
Upstream Interfaces :Gi0/3(Down)
Downstream Interfaces : Gi0/1(Down) Gi0/2(Down)

Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :

(Up):Interface up   (Down):Interface Down   (Dis):Interface disabled
```

Run the **show link state group** command to check whether the link tracking group is created on Device C.

```
DeviceC# show link state group
Link State Group:1  Status: enabled, Down
Upstream Interfaces :Gi0/3(Down)
Downstream Interfaces : Gi0/1(Down) 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

- Device B configuration file

```
hostname DeviceB
!
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
```

- Device C configuration file

```
hostname DeviceC
!
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 6

1.2.3 Procedure 6

1.3 Monitoring 7

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 12

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. VLAN Loop Failure

A VLAN loop failure occurs when all the interfaces in a link loop belong to the same VLAN, forming a loop on the VLAN and causing a broadcast storm. Because the allowed VLAN varies on different device interfaces, a VLAN loop failure may occur within certain VLANs, while traffic can be forwarded normally among other VLANs.

5. Protocol Packets

RLDP defines the following four types of packets:

- Probe 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 probe 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.
- VLAN loop packets (VLAN LOOP): RLDP VLAN loop packets are Layer 2 multicast packets used for VLAN loop detection. Such packets are received only by the sender and are encapsulated in the SNAP format. To

distinguish them from Loop packets, VLAN loop packets carry the VLAN tag.

6. Detection Interval

A detection interval and the maximum detection count can be configured for RLDP. A detection interval determines the period of sending probe packets and loop packets. When a device receives a probe 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 probe 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 probe 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 probe 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 probe 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 probe packet and response packet from the neighbor, it is considered that a bidirectional link failure occurs.

7. 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 probe 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.

8. 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	warning	Only the relevant system log is printed to indicate the failed port and the failure type.

Type	Associated Action/ Recovery Method	Description
failure	Shutdown SVI	A system log is printed. If the failed port is a Layer 2 Ethernet interface or member port of a Layer 2 link aggregation, 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.
	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.
	isolate-vlan	The loop VLAN is isolated in addition to printing a syslog, and the interface does not forward packets received from the isolated VLAN.
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 probe packets exchanged with the neighbor, and link detection is restarted.

9. 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 probe packets, echo packets, or loop packets with the neighbor device. Figure 1-1 shows the protocol states.

Figure 1-1 RLDP Protocol State Diagram

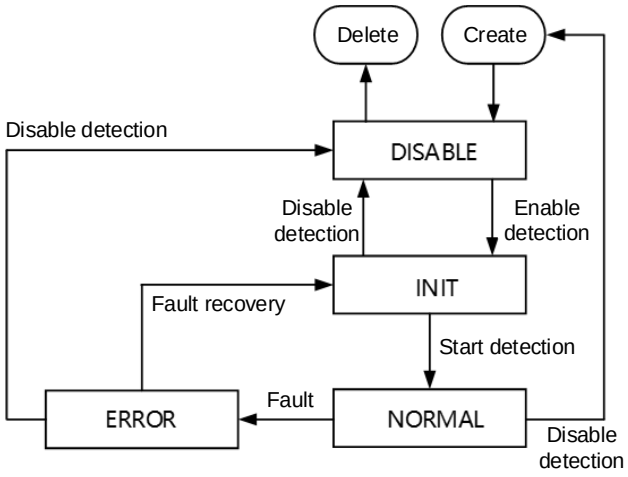


Figure 1-1 shows the detection logic of RLDP, which can be mainly in four states. The four states are described in Table 1-3.

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

The RLDP link detection mode includes unidirectional and bidirectional link detection, downlink detection, and VLAN loop detection.

1. Unidirectional Link Detection

After unidirectional link detection is enabled, a port sends probe packets and receives echo packets from a neighbor regularly. It also receives probe packets from the neighbor and replies with echo packets to the neighbor. If the port receives only probe 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 probe packets and receives echo packets from a neighbor regularly. It also receives probe packets from the neighbor and replies with echo packets to the neighbor. If the port receives neither probe 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 Layer 3 Ethernet interfaces or member ports of a Layer 3 link aggregation; the transmission and receiving ports of packets are Layer 2 interfaces or member ports of a Layer 2 link aggregation, 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.

4. RLDP VLAN Loop Detection

After VLAN loop detection is enabled, the interface periodically sends loop detection packets. Different from RLDP downlink loop detection, this function periodically sends packets with a tag within the VLAN of the interface to check whether the packet returns to the device (the sending interface and receiving interface can be different) to determine whether there is a loop between the interface and the downstream network or device or between the two interfaces of the device. If a loop is detected in a VLAN, RLDP sets the interface into controlled state based on the user configuration and stops loop detection in this VLAN to lower the impact on the device and the network.

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.
- You can configure the RLDP function for interfaces, choose unidirectional, bidirectional, downlink loop detection, or VLAN loop detection, and specify the 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*.

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 Layer 2 Ethernet 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.

(11) Configure RLDP VLAN loop detection for the port.

rldp port vlan-loop-detect { **isolate-vlan** | **warning** } **vlan** *vlan-list*

RLDP VLAN loop detection is not configured for the 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

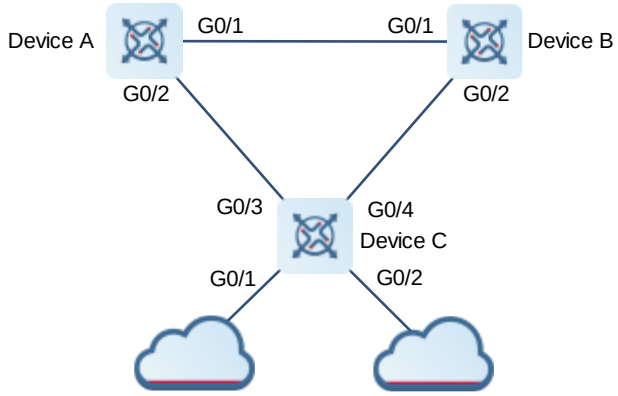
1.4.1 Configuring Basic Features of RLDP

1. Requirements

Aggregation and access use a ring network topology. STP is enabled for all devices on the ring network to prevent loops and provide redundancy protection. To prevent unidirectional or bidirectional link faults in the loop which may invalidate the STP protocol, enable unidirectional and bidirectional RLDP detection between aggregation devices and between aggregation devices and access devices. To prevent loops caused by incorrect downlink connections of aggregation devices, enable RLDP downlink loop detection or VLAN-based loop detection for the downlink interfaces of aggregation and access devices. To prevent loops caused by incorrect downlink connections of access devices, enable RLDP downlink loop detection or VLAN-based loop detection for the downlink interfaces of access devices.

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.

```
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
DeviceA(config-if-GigabitEthernet 0/1)# rldp port bidirection-detect shutdown-port
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# rldp port unidirection-detect shutdown-port
DeviceA(config-if-GigabitEthernet 0/2)# rldp port bidirection-detect shutdown-port
DeviceA(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port
```

Perform the following configuration on device B.

```
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
DeviceB(config-if-GigabitEthernet 0/1)# rldp port bidirection-detect shutdown-port
```

```
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface GigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# rldp port unidirection-detect shutdown-port
DeviceB(config-if-GigabitEthernet 0/2)# rldp port bidirection-detect shutdown-port
DeviceB(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port
```

Perform the following configuration on device C.

```
DeviceC# configure terminal
DeviceC(config)# rldp enable
DeviceC(config)# interface GigabitEthernet 0/3
DeviceC(config-if-GigabitEthernet 0/3)# rldp port unidirection-detect shutdown-port
DeviceC(config-if-GigabitEthernet 0/3)# rldp port bidirection-detect shutdown-port
DeviceC(config-if-GigabitEthernet 0/3)# exit
DeviceC(config)# interface GigabitEthernet 0/4
DeviceC(config-if-GigabitEthernet 0/4)# rldp port unidirection-detect shutdown-port
DeviceC(config-if-GigabitEthernet 0/4)# rldp port bidirection-detect shutdown-port
DeviceC(config-if-GigabitEthernet 0/4)# exit
DeviceC(config)# interface GigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
DeviceC(config-if-GigabitEthernet 0/1)# exit
DeviceC(config)# interface GigabitEthernet 0/2
DeviceC(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.

```
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
bidirection detect information:
    action: shutdown-port
    state : normal

Interface GigabitEthernet 0/2
port state      : normal
neighbor bridge : 00d0.f800.41b0
```

```
neighbor port    : GigabitEthernet 0/3
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 Layer 3 interface.
- 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.
- Ensure that the VLAN is an allowed VLAN of other interfaces when enabling loop detection for it. Otherwise, VLAN loop detection packets cannot be forwarded, causing VLAN loop detection to fail.

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 IPv4 Detection 4

1.4.2 Configuring DLDP IPv6 Detection 5

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.

DLDP IPv4 and DLDP IPv6 always use the same detection mode.

2. Inter-Network Segment Detection

If DLDP needs to check whether an IP address in a network segment that is not directly connected is reachable, the next-hop IP address of the interface must be configured, so DLDP IPv4 can obtain the next-hop MAC address through ARP packets, and DLDP IPv6 can obtain the next-hop MAC address through ND packets and correctly encapsulate and send ICMP packets. 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 Layer 3 interfaces. After the DLDP function is enabled, DLDP IPv4 obtains the MAC address and egress interface of the detected device or the next-hop device for reaching the detected device from ARP packets, and DLDP IPv6 does it from ND packets and performs pathway detection through periodic IPv4 ICMP Echo packets. 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 Layer 3 interfaces.

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 Layer 3 Ethernet interface configuration mode.

interface *interface-type interface-number*

(4) Enable DLDP detection.

dldp { *ipv4-address* [*next-hop-ipv4-address*] | *ipv6-address* [*next-hop-ipv6-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.

This configuration takes effect on both DLDP IPv4 and DLDP IPv6.

(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.

This configuration takes effect immediately for the detection interval of all DLDP detections (DLDP IPv4 and DLDP IPv6).

(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**.

This configuration takes effect immediately for the number of retries of all DLDP detections (DLDP IPv4 and DLDP IPv6).

(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**.

This configuration takes effect immediately for the number of link recovery times of all DLDP detections (DLDP IPv4 and DLDP IPv6).

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* | *ipv6-address*]]	Clears the statistics on link up/down counts of a DLDP monitoring point.
show dldp [**ipv6**] [**interface** *interface-type interface-number*]	Displays the configuration of a DLDP monitoring point.
show dldp [**pv6**] [**interface** *interface-type interface-number*] [**statistic**]	Displays the statistics of a DLDP monitoring point.

1.4 Configuration Examples

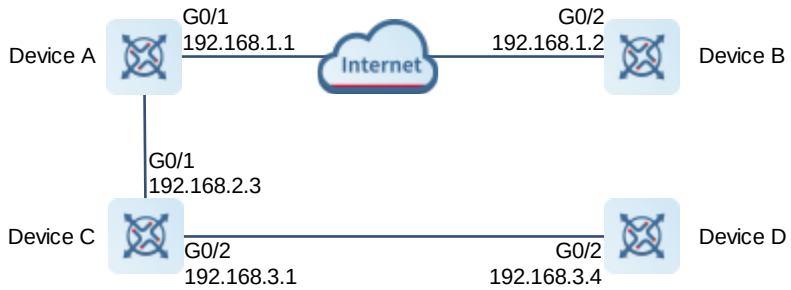
1.4.1 Configuring DLDP IPv4 Detection

1. Requirements

DLDP detection needs to be enabled on an L3 network to control the Layer 3 interfaces of devices A and B.

2. Topology

Figure 1-1 DLDP Topology



3. Notes

- Enable DLDP detection on the Layer 3 interfaces (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 Layer 3 interfaces (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.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# dldp 192.168.1.2
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)# ip address 192.168.2.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# dldp 192.168.3.4 192.168.2.3
```

Perform the following configuration on device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# no switchport
DeviceB(config-if-GigabitEthernet 0/2)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/2)# dldp 192.168.1.1
DeviceB(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.

```
DeviceA# show dldp
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/1     Active   192.168.1.2  0.0.0.0      100      4     3      Up
Gi0/1     Active   192.168.3.4  192.168.2.3  100      4     3      Up
```

```
DeviceB# show dldp
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/2     Passive  192.168.1.1   0.0.0.0       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 IPv4 address is configured for inter-network segment DLDP detection.

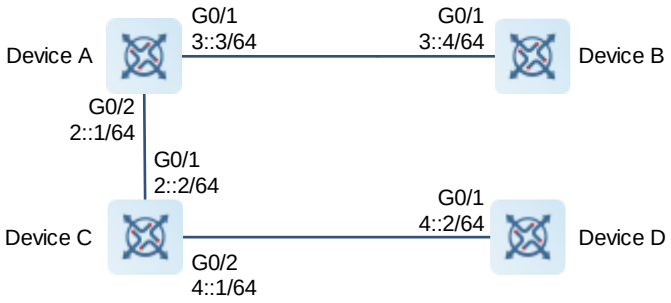
1.4.2 Configuring DLDP IPv6 Detection

1. Requirements

DLDP detection needs to be enabled on an L3 network to control the Layer 3 interfaces of devices A and B.

2. Topology

Figure 1-2 DLDP IPv6 topology



3. Notes

- Enable DLDP detection on the Layer 3 interfaces (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 Layer 3 interfaces (GigabitEthernet 0/1) of device B, enable DLDP detection and configure passive mode on the port.

4. Procedure

Perform the following configuration on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# dldp 3::4
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# dldp 4::2 2::2
```

Perform the following configuration on device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# dldp 3::3
DeviceB(config-if-GigabitEthernet 0/1)# 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.

```
DeviceA# show dldp
Interface  Type        Ipv6       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/1      Active   3::4         ::     100      4     3      Up
Gi0/1      Active   4::2       2::2     100      4     3      Up
```

```
DeviceB# show dldp
Interface  Type        Ip       Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
```

```
Gi0/1      Passive  3::3       ::       100      4      3      Up
```

6. Common Errors

- An unreachable IPv6 unicast route is misjudged as a DLDP detection failure.
- DLDP detection fails because the peer device does not support ARP/ICMPv6 replies.
- No next-hop IPv6 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 10
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 14
1.5.1 Overview 14
1.5.2 Restrictions and Guidelines 14
1.5.3 Procedure 14
1.6 Configuring IPv4 VRRP Tracking 15
1.6.1 Overview 15

1.6.2 Restrictions and Guidelines 15
1.6.3 Procedure 15
1.7 Configuring IPv6 VRRP Tracking 16
1.7.1 Overview 16
1.7.2 Restrictions and Guidelines 16
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 18
1.8.4 Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port 19
1.8.5 Configuring the Dual-Active Mode for an IPV4 VRRP Group 20
1.8.6 Configuring the IPv4 VRRP Packet Version 20
1.9 Monitoring 21
1.10 Configuration Examples 23
1.10.1 Configuring IPv4 VRRP 23
1.10.2 Configuring VRRP + MSTP 28

1 Configuring VRRP

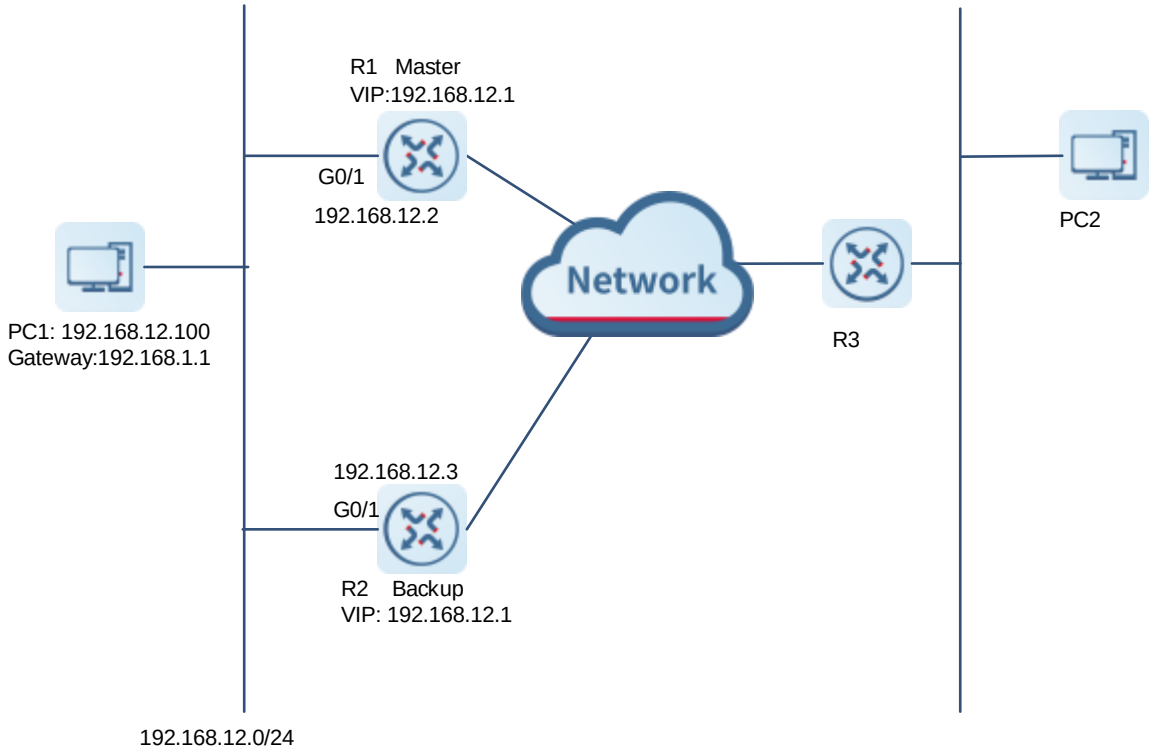
1.1 Introduction

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol, which is mainly used for router redundancy on the egress of a local area network (LAN). VRRP adopts the active/standby mode. When a device used for routing and forwarding on a LAN fails, the backup device automatically takes over the forwarding tasks, 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.

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 device running VRRP. The device can be a single device or a logical device virtualized from multiple devices.

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. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. Priority

The priority of each device in a VRRP group determines the role that each device plays. 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.

10. Preemption Mode

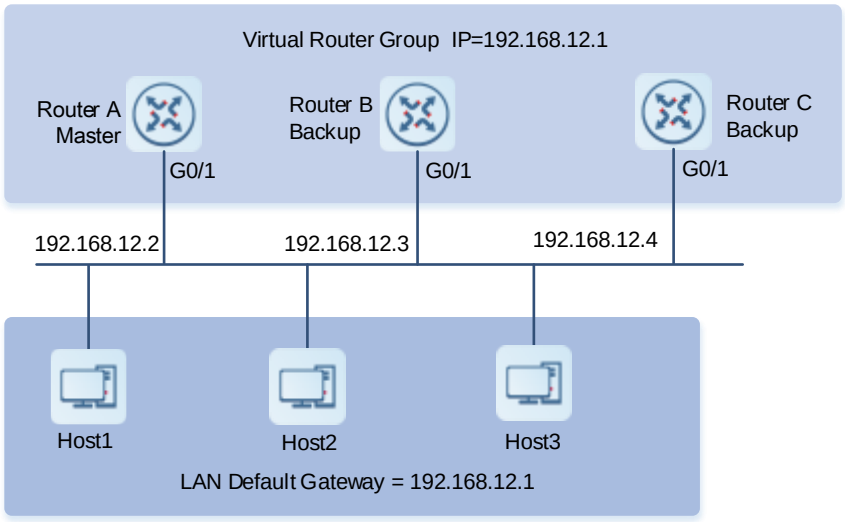
If a VRRP backup group runs in preemption mode, a backup router with a higher priority replaces the master router with a lower priority to become the master router of the VRRP backup group. If the VRRP backup group runs in the non-preemption mode, as long as the master router runs properly, the backup 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

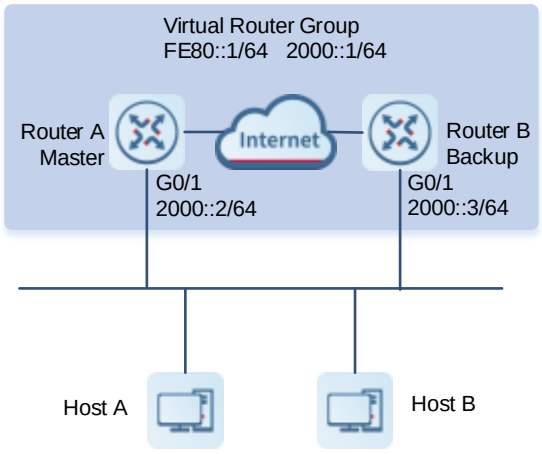
1. Master/Backup Redundancy

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

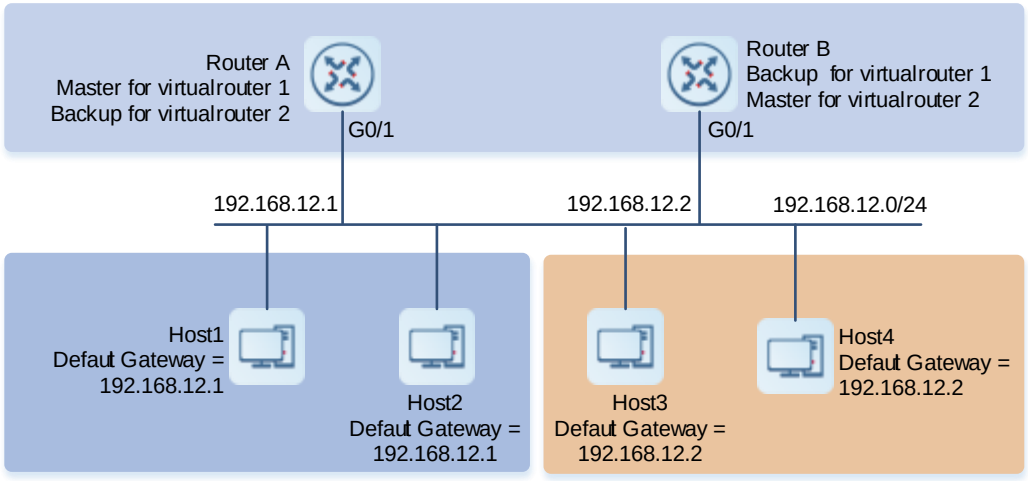


As shown in Figure 1-3, both routers A and B are connected to the LAN through Ethernet ports, and IPv6 VRRP is configured on the Ethernet ports connected to the LAN. The routers are in the same IPv6 VRRP backup group, and the virtual IPv6 addresses of the IPv6 VRRP backup group are FE80::1/64 and 2000::1/64. 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.

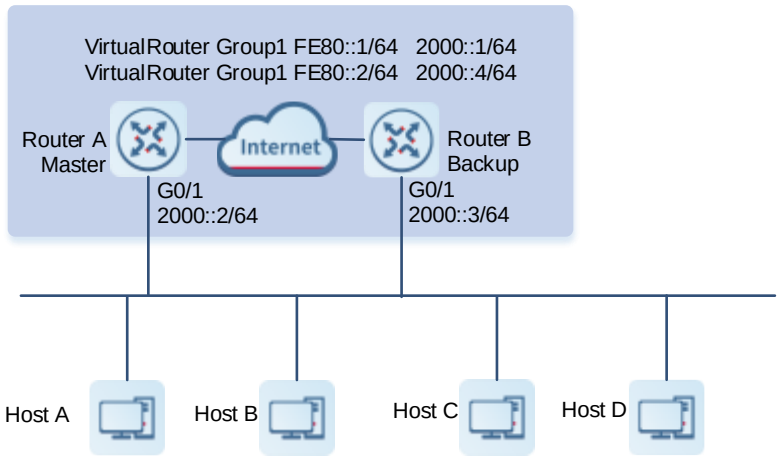
2. Load Balancing

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

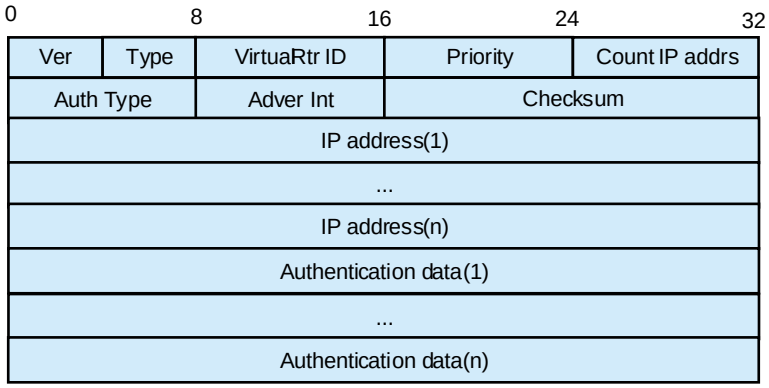


Figure 1-7 Structure of VRRPv3 Packets

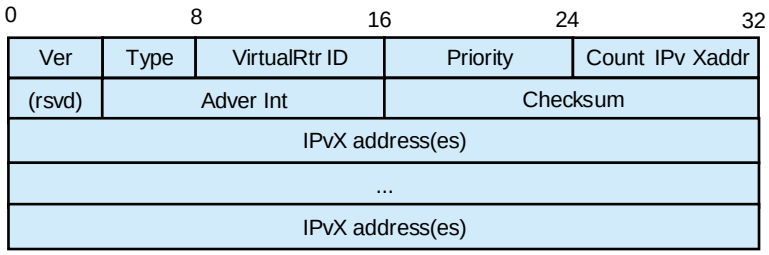


Table 1-1 Fields of VRRP Packets and Description

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)	The Virtual Rtr ID field identifies the virtual router this packet is reporting status for.. The value range is from 1 to 255.	The Virtual Rtr ID field identifies the virtual router this packet is reporting status for. The value range is from 1 to 255.

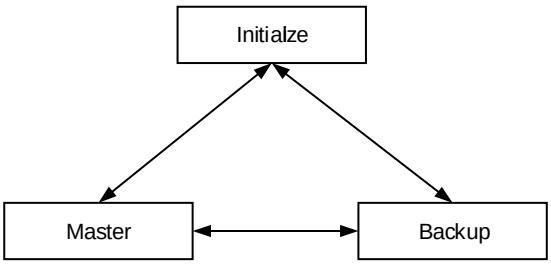
Packet Field	Description	
	VRRPv2	**VRRPv3**
Priority	Priority of the router in the backup group. The value range is from 0 to 255, and the default value is **100**. A larger value indicates a higher priority. When the priority is 0, the current master node no longer joins the VRRP backup group and the 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.	-
Adver Int	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.
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.	-

Packet Field	Description	
	VRRPv2	VRRPv3
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, or a loopback 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

- RFC 2338: Virtual Router Redundancy Protocol
- RFC 3768: Virtual Router Redundancy Protocol (VRRP)
- RFC 5798: 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.

To prevent illegal users from building packets to attack the backup group, you can add authentication words in VRRP packets to verify received VRRP packets. VRRP provides the following authentication modes:

- **md5**: The sending router uses the authentication word and MD5 algorithm for digest operation of VRRP packets and stores the result in the Authentication Header. The receiving router performs the same operation based on the authentication word and MD5 algorithm and compares the result with that in the Authentication Header. If they are the same, the received VRRP packet is legal; otherwise, the received packet is illegal.
- **simple**: The sending router adds the authentication word to the VRRP packet. The receiving router compares the authentication word in the received packet with the local authentication word. If they are the same, the received VRRP packet is legal; otherwise, the received packet is illegal.

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.
- When enabling MD5 authentication for a batch of VRRP groups, run the **vrrp timers advertise** command to increase the interval. Otherwise, the session may be unstable.
- The two authentication modes are subject to the **service password-encryption** command. If the **service password-encryption** command is globally configured:
  - If the **vrrp** *group-id* **authentication simple 0** *key* command is configured, this command is displayed as ciphertext of **vrrp** *group-id* **authentication simple 7** *key*, that is, the simple plaintext is converted into simple ciphertext for storage.
  - If the **vrrp** *group-id* **authentication md5 0** *key* command is configured, this command is displayed as ciphertext of **vrrp** *group-id* **authentication md5 7** *key*.
- The **vrrp** *group-id* **authentication** *key* command is always displayed as simple plaintext. That is, regardless of whether the service password-encryption command is configured, the **vrrp** *group-id* **authentication** *key* command is always displayed as simple plaintext in the echo of the **show running-config** command.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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** [{ **md5** | **simple** } { **0** | **7** }] ke*y*

The authentication mode and word for IPv4 VRRP packets are not 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 interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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, or a loopback 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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** *ipv4-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 ipv4-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, or a loopback 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *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 linkage between IPv6 VRRP groups and BFD.

vrrp ipv6 *group-id* **bfd** *ipv6-address*

Linkage between IPv6 VRRP groups and BFD is not configured on the interface by default.

(8) Exit the global configuration mode.

exit

(9) Configure global IPv6 VRRP BFD.

vrrp ipv6 bfd *interface-type interface-number ipv6-address*

Global BFD is not configured to check whether the Master is in active state for IPv6 VRRP by default.

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) (Optional) Configure VRRP to add the IP packet header and authentication header to the authentication field when using the MD5 algorithm. This step can be performed only for VRRPv2.

vrrp authentication md5 with-ip-auth-header

(4) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode.

  interface vlan *interface-number*

(5) 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 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 interfaces.
- If VRRP and VRRP plus are both enabled on a super VLAN interface, VRRP packets are sent to all the up sub-VLAN interfaces of the super VLAN interface.

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 configuration mode.

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) Enter the SVI configuration mode.

interface vlan *vlan-id*

(7) 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 an SVI.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the SVI configuration 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) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

(4) 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 [**brief** | *group-id*]	Displays the brief or detailed information of IPv4 VRRP.
show vrrp interface *interface-type interface-number* [**brief**]	Displays the information of an IPv4 VRRP group on a specified port.
show [**ipv6**] **vrrp bfd-neighbor**	Displays the association between the VRRP and BFD.

Command	Purpose
show vrrp client [[**pid** *pid*] **brief** | **reset**]	Displays information about clients connected to the VRRP server.
show vrrp jemalloc-statistic	Displays detailed Jemalloc information about the VRRP software.
show vrrp log { **dbg** | **error** | **init** }	Displays the VRRP log files.
show vrrp memory	Displays the memory information of a VRRP process.
show vrrp mom	Displays the exchange information between the VRRP and the MOM.
show vrrp packet statistics [*interface-type interface-number* | **total**]	Displays the statistics of VRRP packets.
show vrrp server-statistic [**reset**]	Displays the statistics of the VRRP server.
show [**ipv6**] **vrrp work-state** [**interface** *interface-name interface-type* [*vrrp-group-id*]]	Displays the current detailed status of the VRRP group.
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.
debug vrrp	Debugs VRRP errors, events, packets, and state.
debug vrrp errors	Debugs VRRP errors.
debug vrrp events	Debugs VRRP events.
debug vrrp packets [**acl** *acl-id* **|** [**icmp** | **protocol**] **interface** *interface-type interface-number* [*group-id*]]	Debugs VRRP packets.
debug vrrp state	Debugs VRRP state.

1.10 Configuration Examples

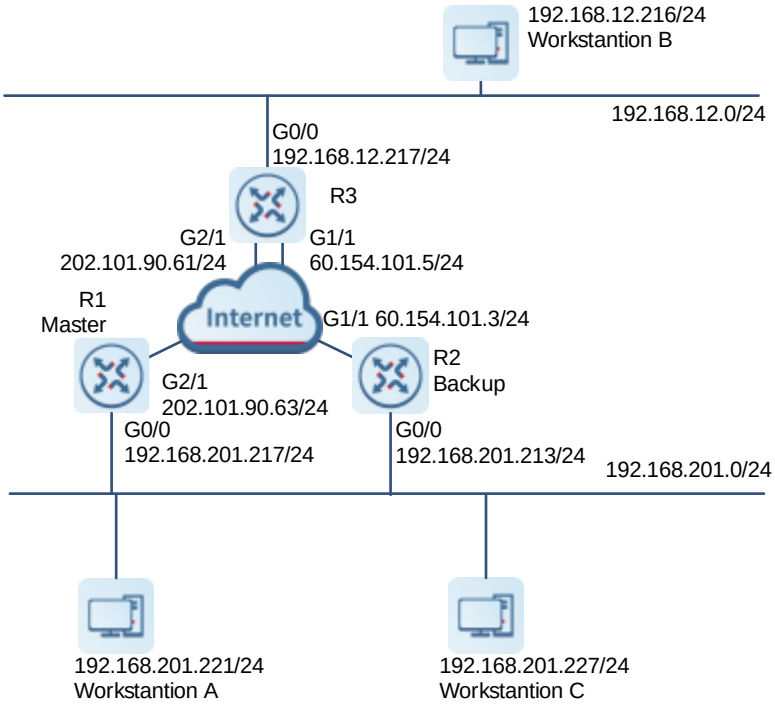
1.10.1 Configuring IPv4 VRRP

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

Configure R1.

(1) Configure an interface address.

```
R1> enable
R1# configure terminal
R1(config)# interface gigabitEthernet 0/1
```

```
R1(config-if-GigabitEthernet 0/1)# no switchport
R1(config-if-GigabitEthernet 0/1)# ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/1)# exit
R1(config)# interface gigabitEthernet 0/2
R1(config-if-GigabitEthernet 0/2)# no switchport
R1(config-if-GigabitEthernet 0/2)# ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 0/2)# exit
```

(2) Configure OSPF routes to ensure Layer 3 reachability between devices.

```
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
R1(config-router)# exit
```

(3) Configure VRRP on GigabitEthernet 0/1.

Set the VRRP priority to 120.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# vrrp 1 priority 120
```

Set the interval for a VRRP group to send VRRP advertisements to 3 seconds.

```
R1(config-if-GigabitEthernet 0/1)# vrrp 1 timers advertise 3
```

Set the ID of a VRRP group to 1 and virtual address to 192.168.201.1.

```
R1(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.201.1
```

Configure GigabitEthernet 0/2 as a monitored port of a VRRP group and configure the VRRP priority to change to 30 when the link state of the monitored port changes.

```
R1(config-if-GigabitEthernet 0/1)# vrrp 1 track GigabitEthernet 0/2 30
R1(config-if-GigabitEthernet 0/1)# exit
```

Configure R2.

(4) Configure an interface address.

```
R2> enable
R2# configure terminal
R2(config)# interface GigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# no switchport
R2(config-if-GigabitEthernet 0/1)# ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/1)# exit
R2(config)# interface GigabitEthernet 0/2
R2(config-if-GigabitEthernet 0/2)# no switchport
R2(config-if-GigabitEthernet 0/2)# ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 0/2)# exit
```

(5) Configure OSPF routes to ensure Layer 3 reachability between devices.

```
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
```

(6) Set the ID of a VRRP group to 1 and virtual address to 192.168.201.1.

Set the ID of a VRRP group to 1 and virtual address to 192.168.201.1.

```
R2(config-if-GigabitEthernet 0/1)# vrrp 1 ip 192.168.201.1
```

Set the interval for a VRRP group to send VRRP advertisements to 3 seconds.

```
R2(config-if-GigabitEthernet 0/1)# vrrp 1 timers advertise 3
```

Configure R3.

(7) Configure an interface address.

```
R3> enable
R3# configure terminal
R3(config)# interface GigabitEthernet 0/1
R3(config-if-GigabitEthernet 0/1)# no switchport
R3(config-if-GigabitEthernet 0/1)# ip address 192.168.12.217 255.255.255.0
R3(config-if-GigabitEthernet 0/1)# exit
R3(config)# interface GigabitEthernet 0/2
R3(config-if-GigabitEthernet 0/2)# no switchport
R3(config-if-GigabitEthernet 0/2)# ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 0/2)# exit
R3(config)# interface GigabitEthernet 0/3
R3(config-if-GigabitEthernet 0/3)# no switchport
R3(config-if-GigabitEthernet 0/3)# ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 0/3)# exit
```

(8) Configure OSPF routes to ensure Layer 3 reachability between devices.

```
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
```

5. Verification

(1) Run the **show vrrp** command to verify the configuration.

Configure R1 as the master router.

```
R1# show vrrp
GigabitEthernet 0/1 - 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 0/2 priority decrement=30
```

Configure R2 as the backup router.

```
R2#show vrrp
```

```
GigabitEthernet 0/1 - 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
```

(2) When GigabitEthernet 0/2 of R1 used to connect to the WAN is unavailable, the priority of R1 in the VRRP group is decreased by 30 to 90. In this case, R2 becomes the master router.

```
R1# show vrrp
GigabitEthernet 0/1 - 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 100
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

(3) When GigabitEthernet 0/2 of R1 connected to the WAN changes to Up, the priority of R1 in the VRRP group is increased by 30 to 120, and R1 becomes the master router again.

```
R1# show vrrp
GigabitEthernet 0/1 - 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 0/2 priority decrement=30
```

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.

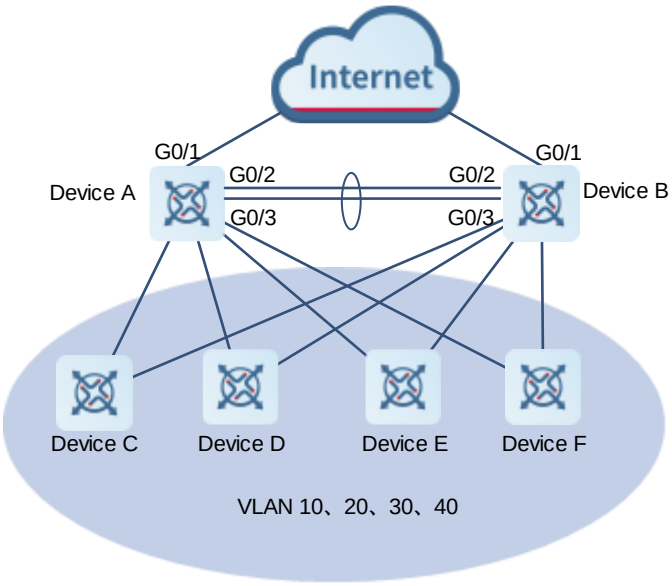
1.10.2 Configuring VRRP + MSTP

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 (devices 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 (devices 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
Device A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Device B		192.168.10.3			Backup
Device A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Device B		192.168.20.3			Backup
Device A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Device B		192.168.30.3			Master
Device A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Device B		192.168.40.3			Master

- Configure the uplink ports (port GigabitEthernet 0/1 of devices 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 devices 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 devices A and B.
- Configure device A as the root bridge of MST 0 and MST 1, and device 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 of the VRRP groups.
- Configure the interconnected ports of the core routers as a Layer 2 link aggregation.

4. Procedure

(1) Perform the following configuration on Device A:

Create VLANs 10, 20, 30, and 40.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan range 10,20,30,40
DeviceA(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.

```
DeviceA(config)# spanning-tree mst configuration
DeviceA(config-mst)# instance 1 vlan 10,20
DeviceA(config-mst)# instance 2 vlan 30,40
DeviceA(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**.

```
DeviceA(config)# spanning-tree mst 0 priority 4096
DeviceA(config)# spanning-tree mst 1 priority 4096
DeviceA(config)# spanning-tree mst 2 priority 8192
```

Enable MSTP.

```
DeviceA(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.

```
DeviceA(config)# interface vlan 10
DeviceA(config-if-VLAN 10)# ip address 192.168.10.2 255.255.255.0
DeviceA(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
DeviceA(config-if-VLAN 10)# exit
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 30
DeviceA(config-if-VLAN 30)# ip address 192.168.30.2 255.255.255.0
DeviceA(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
DeviceA(config-if-VLAN 30)# 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
```

Increase the priority of backup groups 10 and 20 on switch A to **120**.

```
DeviceA(config)# interface vlan 10
DeviceA(config-if-VLAN 10)# vrrp 10 priority 120
DeviceA(config-if-VLAN 10)# exit
DeviceA(config)# interface vlan 20
DeviceA(config-if-VLAN 20)# vrrp 20 priority 120
DeviceA(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.

```
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no switchport
DeviceA(config-if-GigabitEthernet 0/1)# ip address 10.10.1.1 255.255.255.0
DeviceA(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.

```
DeviceA(config)# interface vlan 10
DeviceA(config-if-VLAN 10)# vrrp 10 track gigabitEthernet 0/1 30
DeviceA(config-if-VLAN 10)# exit
DeviceA(config)# interface vlan 20
DeviceA(config-if-VLAN 20)# vrrp 20 track gigabitEthernet 0/1 30
DeviceA(config-if-VLAN 20)# exit
```

Configure the ports GigabitEthernet 0/2 and GigabitEthernet 0/3 to belong to a Layer 2 link aggregation, and configure the link aggregation as a trunk port.

```
DeviceA(config)# interface range gigabitEthernet 0/2-3
DeviceA(config-if-range)# port-group 1
DeviceA(config)# interface aggregateport 1
DeviceA(config-if-AggregatePort 1)# switchport mode trunk
```

(2) Perform the following configuration on device B:

Create VLANs 10, 20, 30, and 40.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# vlan range 10,20,30,40
DeviceB(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.

```
DeviceB(config)# spanning-tree mst configuration
DeviceB(config-mst)# instance 1 vlan 10,20
```

```
DeviceB(config-mst)# instance 2 vlan 30,40
DeviceB(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**.

```
DeviceB(config)# spanning-tree mst 2 priority 4096
DeviceB(config)# spanning-tree mst 0 priority 8192
DeviceB(config)# spanning-tree mst 1 priority 8192
```

Enable MSTP.

```
DeviceB(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.

```
DeviceB(config)# interface vlan 10
DeviceB(config-if-VLAN 10)# ip address 192.168.10.3 255.255.255.0
DeviceB(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
DeviceB(config-if-VLAN 10)# exit
DeviceB(config)# interface vlan 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)# exit
DeviceB(config)# interface vlan 30
DeviceB(config-if-VLAN 30)# ip address 192.168.30.3 255.255.255.0
DeviceB(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
DeviceB(config-if-VLAN 30)# 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)# exit
```

Increase the priority of VRRP 30 and VRRP 40 on Device B to **120**.

```
DeviceB(config)# interface vlan 30
DeviceB(config-if-VLAN 30)# vrrp 30 priority 120
DeviceB(config-if-VLAN 30)# exit
DeviceB(config)# interface vlan 40
DeviceB(config-if-VLAN 40)# vrrp 40 priority 120
DeviceB(config-if-VLAN 40)# exit
```

Configure the port GigabitEthernet 0/1 of Device B as a route port, and set the IP address to 10.10.2.1/24.

```
DeviceB(config)#interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# no switchport
DeviceB(config-if-GigabitEthernet 0/1)# ip address 10.10.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure the port GigabitEthernet 0/1 of Device B as the monitored port of backup groups 30 and 40, and set *Priority decrement* to 30.

```
DeviceB(config)# interface vlan 30
DeviceB(config-if-VLAN 30)# vrrp 30 track gigabitEthernet 0/1 30
DeviceB(config-if-VLAN 30)# exit
```

```
DeviceB(config)# interface vlan 40
DeviceB(config-if-VLAN 40)# vrrp 40 track gigabitEthernet 0/1 30
DeviceB(config-if-VLAN 40)# exit
```

Configure the ports GigabitEthernet 0/2 and GigabitEthernet 0/3 to belong to a Layer 2 link aggregation, and configure the link aggregation as a trunk port.

```
DeviceB(config)# interface range gigabitEthernet 0/2-3
DeviceB(config-if-range)# port-group 1
DeviceB(config)# interface aggregateport 1
DeviceB(config-if-AggregatePort 1)# switchport mode trunk
```

5. Verification

(1) Run the **show vrrp brief** commands to check whether the configuration is correct.

- Check the VRRP state of device A.

```
DeviceA# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.2  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
```

- Check the VRRP state of device B.

```
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   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
```

(2) Disconnect the uplink of switch A and run the **show vrrp brief** commands to check the VRRP state of the device.

```
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   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
```

(3) Disconnect the uplink of device B and run the **show vrrp brief** commands to check the VRRP state of the device.

```
DeviceB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.3  192.168.20.1
VLAN 30    30   90   3      -    P    Backup  192.168.30.3  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

```
hostname DeviceA
!
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
```

- Device B configuration file

```
hostname DeviceB
!
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 5
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

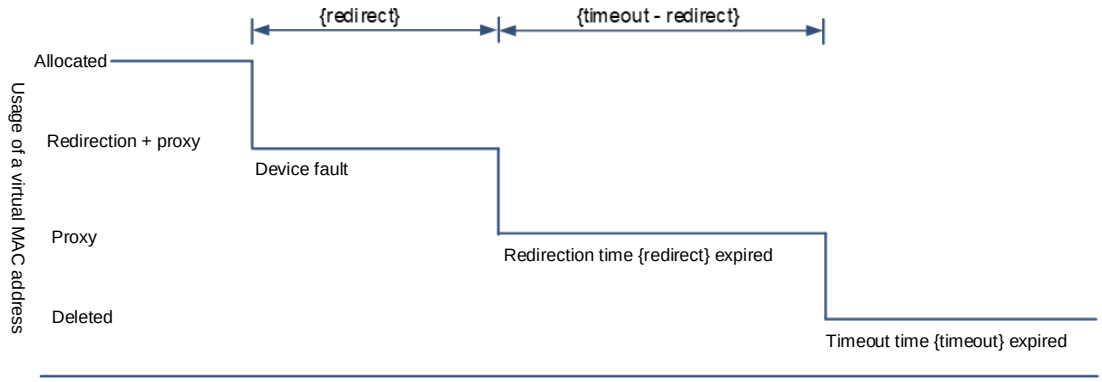
the virtual MAC address. In addition, this proxy device takes over traffic of original hosts to prevent traffic interruption. The virtual MAC address allocated to a device in a backup group can be called a master virtual MAC address, and the virtual MAC address used by this device on behalf of another 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

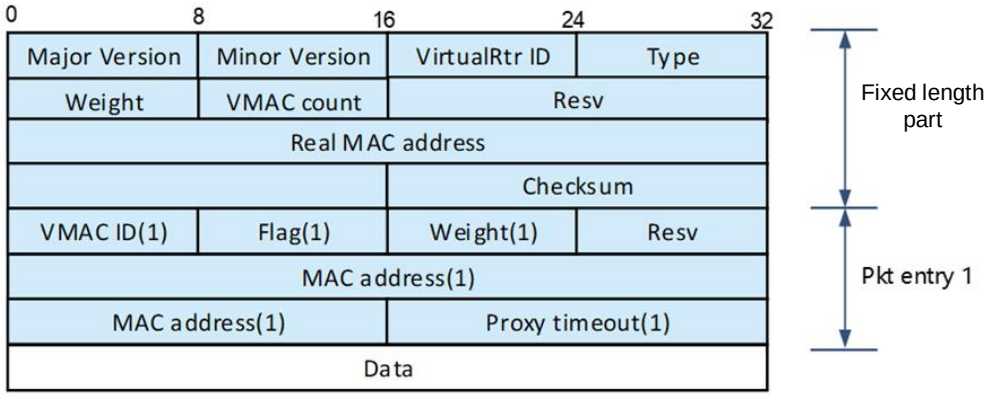


Table 1-1 Field Description of VRRP Plus Packets

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 interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the switch virtual interface (SVI) configuration mode.

  interface vlan *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** [*group-id* | [**interface** *interface-type interface-number*] **brief**]	Displays the information about VRRP Plus.
show [**ipv6**] **vrrp balance bfd-neighbor**	Displays the association between VRRP Plus and BFD.
show vrrp balance debug-logging	Displays the content of VRRP Plus log files.
show vrrp balance jemalloc-statistic	Displays the Jemalloc information of VRRP Plus.
show vrrp balance memory	Displays the memory information of a VRRP Plus process.
show vrrp balance mom-info	Displays the exchange information between VRRP Plus and MOM.
show vrrp balance server-statistic [**reset**]	Displays the VRRP Plus server statistics.
show [**ipv6**] **vrrp balance work-state** [**interface** *interface-type interface-number* [*vrrp-group-id*]]	Displays the current detailed status of the VRRP Plus backup group.

1.5 Configuration Examples

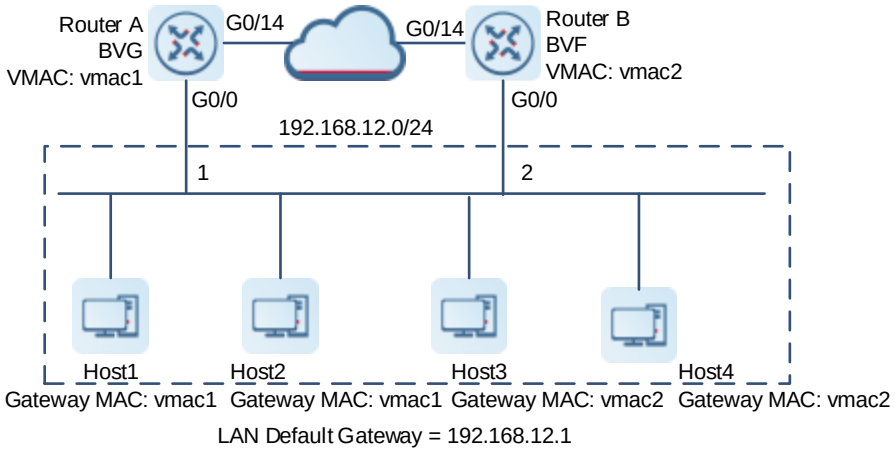
1.5.1 Configuring IPv4 VRRP Plus

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 on Router A to display the configuration of the VRRP Plus backup group. If the backup group has packet forwarding tasks, **local** is displayed in the **Forwarder** field, 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
```

Run the **show vrrp balance** command on Router B to display the configuration of the VRRP Plus backup group. If the backup group has packet forwarding tasks, **local** is displayed in the **Forwarder** field, and the virtual MAC address allocated to this backup group is also displayed.

```
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
```

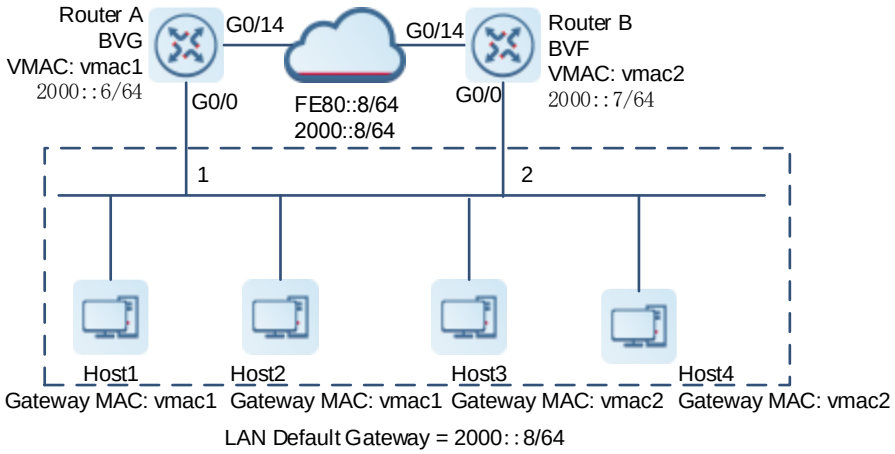
1.5.2 Configuring IPv6 VRRP Plus

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 ipv6 fe80::8
RouterA(config-if-GigabitEthernet 0/0)# vrrp 1 ipv6 2000::8
RouterA(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 priority 120
RouterA(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 balance
RouterA(config-if-GigabitEthernet 0/0)# vrrp ipv6 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)# ipv6 address 2000::7/64
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 ipv6 fe80::8
RouterB(config-if-GigabitEthernet 0/0)# vrrp 1 ipv6 2000::8
RouterB(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 balance
RouterB(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 load-balancing weighted
```

5. Verification

Run the **show vrrp balance** command on Router A to display the configuration of the VRRP Plus backup group. If the backup group has packet forwarding tasks, **local** is displayed in the **Forwarder** field, 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
```

Run the **show vrrp balance** command on Router B to display the configuration of the VRRP Plus backup group. If the backup group has packet forwarding tasks, **local** is displayed in the **Forwarder** field, and the virtual MAC address allocated to this backup group is also displayed.

```
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 6
1.1.6 BFD Flapping Advertisement Dampening 6
1.1.7 Protocols and Standards 6
1.2 Restrictions and Guidelines 7
1.3 Configuration Task Summary 8
1.4 Configuring BFD Basic Functions 8
1.4.1 Overview 8
1.4.2 Configuration Tasks 8
1.4.3 Configuring BFD Parameters 8
1.4.4 Configuring the BFD Slow Timer 9
1.4.5 Configuring BFD Support for L3 Interfaces 9
1.5 Configuring BFD Protection 10
1.5.1 Overview 10
1.5.2 Restrictions and Guidelines 10
1.5.3 Prerequisites 10
1.5.4 Procedure 10
1.6 Configuring BFD Flapping Advertisement Dampening 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 12

1.8.1 Configuring BFD Support for OSPF 12

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 routers. It quickly detects faults on the bidirectional forwarding path between two routers for upper layer protocols such as routing protocols 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

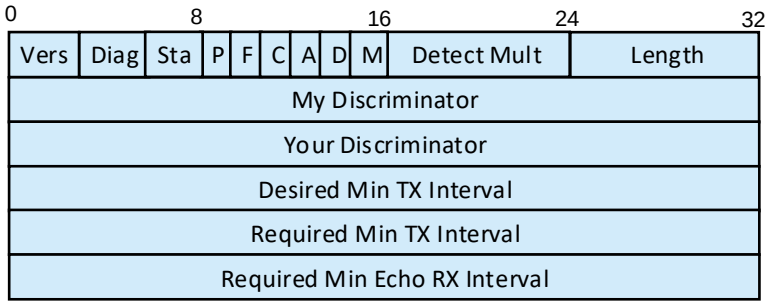


Table 1-1 Description of BFD Packet Fields

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.

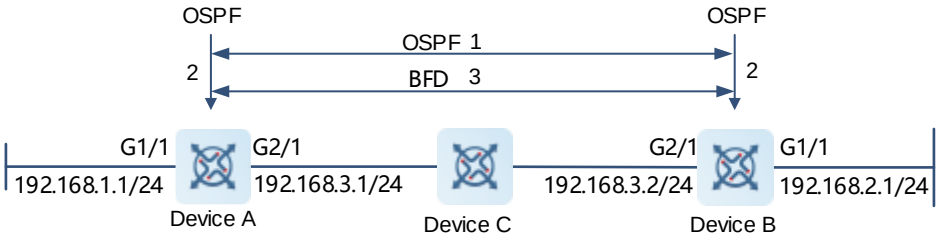
1.1.2 Session Establishment

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 routers running OSPF and BFD are connected through an intermediate network 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.

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.

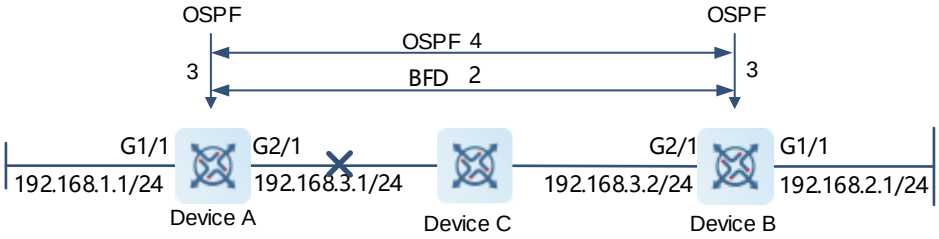
1.1.3 Session Detection

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 routers running OSPF and BFD are connected through an intermediate network device.

Figure 1-3 Topology for BFD Session Detection



The handling process after a BFD session is down is as follows:

- The link between router A and the switch fails.
- The BFD session between routers A and 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.

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 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)

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 Slow Timer
- (Optional) Configuring BFD Support for L3 Interfaces

(2) (Optional) Configuring BFD Protection

(3) (Optional) Configuring BFD Flapping Advertisement Dampening

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 Slow Timer

(3) (Optional) Configuring BFD Support for L3 Interfaces

1.4.3 Configuring BFD Parameters

1. Overview

- Unless otherwise specified, for single-hop sessions, a BFD session should be established between routers 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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *interface-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode

  interface aggregateport *interface-number*

- Enter the Layer 2 aggregate interface configuration mode

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode

  interface vlan *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 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 of switches or routers.
- 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.

1.4.5 Configuring BFD Support for L3 Interfaces

1. Overview

This feature is used to enable BFD support for L3 interfaces so as to rapidly detect connectivity of L3 interfaces.

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) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *interface-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode

  interface vlan *interface-number*

(5) 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.

1.5 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 switch 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) Enter the interface configuration mode.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *interface-type interface-number*

- Enter the Layer 2 aggregate interface configuration mode

  interface aggregateport *interface-number*

- Enter the Layer 3 aggregate interface configuration mode

  interface aggregateport *interface-number*

- Enter the SVI interface configuration mode

  interface vlan *interface-number*

(5) 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 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** | **dhcp** | **isis** | **openflow** | **ospf** | **ospfv3** | **pbr** | **pst** | **rip** | **static-route** | **vrrp** | **vrrp-balance** }] [**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.

1.8 Configuration Examples

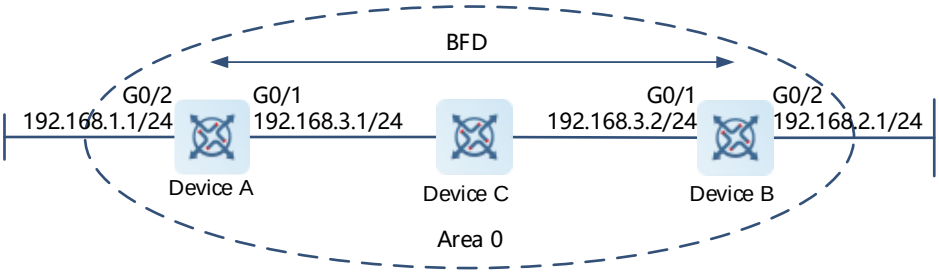
1.8.1 Configuring BFD Support for OSPF

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.

```
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet0/1)# no switchport
DeviceB(config-if-GigabitEthernet0/1)# ip address 192.168.3.2 255.255.255.0
DeviceB(config-if-GigabitEthernet0/1)# bfd interval 200 min_rx 200 multiplier 5
DeviceB(config-if-GigabitEthernet0/1)# exit
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet0/2)# no switchport
DeviceB(config-if-GigabitEthernet0/2)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet0/2)# 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
```

Perform the following configuration on device B.

```
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet0/1)# no switchport
DeviceB(config-if-GigabitEthernet0/1)# ip address 192.168.3.2 255.255.255.0
DeviceB(config-if-GigabitEthernet0/1)# bfd interval 200 min_rx 200 multiplier 5
DeviceB(config-if-GigabitEthernet0/1)# exit
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet0/2)# no switchport
DeviceB(config-if-GigabitEthernet0/2)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet0/2)# 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      Ge0/1
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      Ge0/1
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 Principles 1

1.2 Configuring Track 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 3

1.4.1 Configuring to Track Link Status of Interfaces 3

1.4.2 Configuring to Track the Results of RNS Instances 4

1 Configuring Track

1.1 Introduction

The track module supports monitoring and fault transmission. It connects to the detection module to detect the link status and network performance, and connects to the application module to transmit the detection results of link failure and network performance. In this way, the application module can quickly perceive the changes of the network status and respond in time, thereby preventing communication failures or service quality deterioration.

1.1.1 Principles

Each track instance is used to track one type of monitored object. The status of the track instance reflects the status of the tracked object. When the status of the tracked object changes, the status change can be transmitted to the application module that interoperates with the track instance. Currently, the following objects can be tracked:

- RNS test result.
- Interface link status
- Test result of the RNS list
- Track list status

1.2 Configuring Track

1.2.1 Overview

The track function can be used to track the RNS test results, the interface link status, the track list status, and the status of the RNS test list. The status change of the track object can be advertised to the corresponding application module to enable the application module to quickly perceive the network status change and respond in time.

1.2.2 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.
- A longer delay indicates a lengthier waiting period before notifying the modules monitoring that Track instance of the status.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) 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** }

(4) Configure a track member.

object *object-number* [**not**]

No member object is configured by default.

(5) Configure the notification delay of a track object.

delay { **down** *interval* | **up** *interval* } *

By default, the status of the tracked object is immediately notified upon an Up/Down status change.

1.3 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 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** | **client** | **proc-event** | **rdnd-event** }	Debugs the track module.

1.4 Configuration Examples

1.4.1 Configuring to Track Link Status of 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 1-1 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
```

6. Configuration File

```
track 1 Interface GigabitEthernet 0/0 line-protocol
 delay up 20 down 40
!
track 2 Interface GigabitEthernet 0/1 line-protocol
```

```
 delay down 30
!
track 3 list boolean and
 object 1
 object 2 not
!
```

1.4.2 Configuring to Track the Results of 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
```

5. Configuration File

```
track 5 rns-list 1,2-5,8 and
 delay up 20 down 30
!
```

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.

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.

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 aggregate interface configuration mode.

  interface aggregateport *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 Routers A and 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 a Layer 3 device before the interface is converted to a Layer 3 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

1.4 Monitoring 2

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.

1.4 Monitoring

Run the **show** command to display the configuration.

Command	Purpose
show ham log { **all** | **bad-script** | **error** | **kill** | **multi-instance** | **no-alive** | **reg-alive** | **reg-restart** | **restart** | **running-event** }	Displays the HAM log information.
show ham register { **alive** | **delay-restart** | **fail-chain** | **restart** }	Displays the detailed HAM information of service registration.

Contents

1 SYSHA 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Monitoring 2

1 SYSHA

1.1 Introduction

1.1.1 Overview

On a complex network, the operating system of a device may be exhausted when the device receives and processes a large number of packets, affecting normal service running. SYSHA monitors software resources of devices and provides self-healing upon resource exceptions, preventing long service interruptions.

1.1.2 Principles

1. System Resources

Software resources monitored by SYSHA include the following items.

- CPU usage

  The CPU usage is the ratio of the CPU load to the CPU processing capability, which is expressed in percentage. It indicates the percentage of time that the CPU occupies for processing and computing tasks within a period of time. For example, if the CPU usage is 30%, 30% of the CPU time is used for calculation, and the remaining time is idle.

- File descriptor

  A file descriptor is an index created by the kernel to manage opened files and points to an opened file. The operating system limits the total number of file descriptors that can be used by software. Once the number of file descriptors used by the software exceeds the limit, the software encounters an exception.

- Memory usage

  The memory usage is the ratio of the used memory to the total memory. If the software occupies excessive system memory resources, normal running of other software on the device will be affected.

- Number of threads

  A thread is the smallest unit of an operating system for performing computing and scheduling. It is included in a process and is the operation unit of the process. One process can have multiple threads running concurrently, and each thread runs a different task simultaneously. The operating system allocates a thread ID to each thread, but the total number of thread IDs is limited. Therefore, a process cannot occupy too many thread resources. Otherwise, thread IDs will be exhausted, affecting normal running of other software.

2. Monitoring and Self-healing

SYSHA uses scheduled sampling to monitor the system resource usage of software. At intervals, SYSHA scans and records the system resource usage of software, calculates the average value of multiple rounds, and determines whether the current system resource usage of the process is normal. If SYSHA detects that the software occupies too many device software resources and affects normal operation of services, it will restart the services or the device.

1.2 Monitoring

Run the **show** command to display the configuration.

Table 1-1 SYSHA Monitoring

Command	Purpose
show sysha [**cpu** | **fd** | **memory** | **thread**]	Displays SYSHA information and the resource status.

Network Management and Monitoring Configuration

1. Configuring SNMP
2. Configuring RMON
3. Configuring NETCONF
4. OpenFlow
5. Configuring gRPC
6. Configuring CWMP
7. Configuring SPAN
8. Configuring RNS
9. Configuring sFlow

Contents

1 Configuring SNMP 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 Basic SNMP Features 6
1.3.1 Overview 6
1.3.2 Restrictions and Guidelines 7
1.3.3 Procedure 7
1.4 Configuring the Trap Function 9
1.4.1 Overview 9
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure 9
1.5 Configuring the Agent Shielding Function 11
1.5.1 Overview 11
1.5.2 Restrictions and Guidelines 11
1.5.3 Procedure 11
1.6 Configuring SNMP Control Parameters 12
1.6.1 Overview 12
1.6.2 Restrictions and Guidelines 12
1.6.3 Procedure 12

1.7 Monitoring 13

1.8 Configuration Examples..... 14

1.8.1 Configuring Basic SNMPv2c Function..... 14

1.8.2 Configuring Basic SNMPv3 Function 15

1.8.3 Configuring Basic Trap Function..... 19

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.

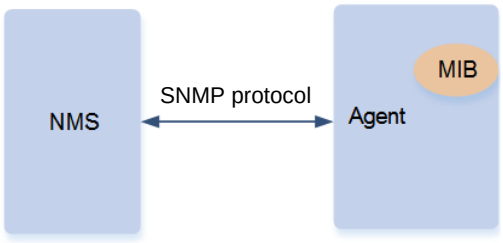
1.1.2 Principles

1. Basic Concepts

The SNMP management system has the following components:

- Network management system (NMS)
- SNMP agent
- MIB

Figure 1-1 Relationship Between the NMS and Network Management Agent



- SNMP network manager

  The NMS controls and monitors the network based on SNMP or is a server that has the network management software deployed.

  The NMS can send SNMP instructions to the SNMP agent to query or modify the parameter values of one or more devices, and receive Trap messages from the SNMP agent to learn the running status of the managed devices.

- 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:

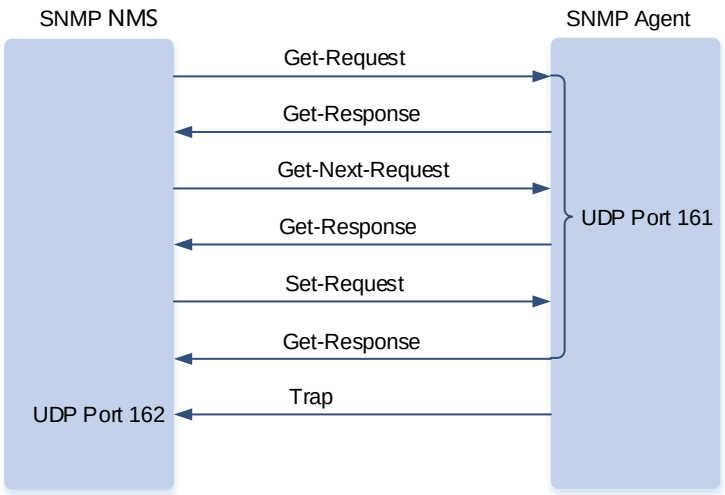
  - Get-Request: The NMS extracts one or more parameter values from the agent.
  - Get-Next-Request: The NMS extracts the parameter value next to one or more parameters from the agent.
  - Get-Bulk: The NMS extracts a batch of parameter values from the agent.
  - Set-Request: The NMS sets one or more parameter 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 the situation happening in the agent.

  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. SNMP Versions

- SNMPv1

  SNMPv1 is the first official version of SNMP and is defined in RFC 1157. Based on community names, SNMPv1 has simple structure of management information (SMI) and simple management information base (MIB) and lower security.

- SNMPv2c

  SNMPv2c is a community-based SNMP management architecture and is defined in RFC 1901. SNMPv2c is compatible with SNMPv1. Compared with SNMPv1, SNMPv2c 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.

4. Principles of SNMPv1 and SNMPv2c

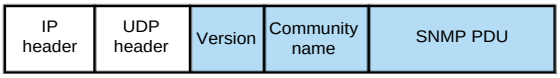
SNMPv1 and SNMPv2c adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

SNMPv1 and SNMPv2c 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.

5. Principles of SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2c into the SNMPv3 system.

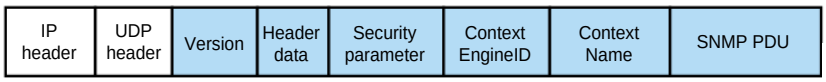
The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications 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 a specified 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. RFC 3411 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.

1.1.3 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 specified 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.
- When SNMPv3 is used to manage network devices, a user must be configured.
- 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 function 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** { *acl-name* | *acl-number* | **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* [**view** *view-name*] [**ro** | **rw**] [**host** *ipv4-address* | **host** *ipv6-address*] [*acl-name* | *acl-number* | **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 { [**remote-engineid** *engineid*] **user** *username group-name* **v3** { [**encrypted**] [**auth** { **md5** | **sha** | **sha2-256** | **sha2-512 | sm3** } *auth-password* [**priv** { **3des | aes128 | des56** | **sm4** } *priv-password*]] | **interactive** [**auth** { **md5** | **sha** | **sha2-256** | **sha2-512 | sm3** } [**priv** { **3des | aes128 | des56** | **sm4** }]] } | **user** *username group-name* { **v1** | **v2c** } } [**access** { *acl-name* | *acl-number* | **ipv6** *ipv6-acl-name* [*acl-name* | *acl-number*] }]

No SNMP user is configured by default.

(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** }

By default, the SNMP attack detection function is enabled, the maximum number of consecutive SNMP authentication failures is 3, and a source IP address can be authenticated again in five minutes after it is prohibited.

(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 { **authentication** { **fail | success** } | **get-operation** | **set-operation** | **trap-info** }

By default, the function of logging the Get and Get-Next Operations performed by the NMS on the SNMP agent is disabled and the function of logging the Set Operation is enabled.

(11) (Optional) Display SNMP help information. All the following configuration tasks are optional. Select the configuration tasks as required.

- Display help information about SNMP.

  snmp-server help

- Display help information about SNMP authentication names and access permissions.

  snmp-server community help

- Display help information about the SNMP user group.

  snmp-server group help

- Display help information about SNMP users.

snmp-server user help

- Display help information about the SNMP view.

  snmp-server view help

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.

Management interface configuration:

snmp-server host [**oob**] { *ipv4-address* | **ipv6** *ipv6-address* | **domain** *domain-name* } [**informs** | **traps**] [**version** { { **1** | **2c** } [**0** | **7**] *community* | **3** { **auth** | **noauth** | **priv** } *username* }] [**udp-port** *port-number*] [**via mgmt** *interface-number*] [*notification-type*]

Non-management interface configuration:

snmp-server host { *ipv4-address* | **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*] [*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 [**authentication all-protocols** | **bgp** | **bridge** | **entity** | **envom** | **isis** | **mac-notification** | **mpls** *mpls-trap* | **nfpp** | **normal** | **ospf** | **running-config-change** | **snmp** [**authentication** | **coldstart** | **heartbeat** | **linkdown** | **linkup** | **warmstart**] * | **startup-config-change** | **urpf** | **vrrp** | **vxlan** | **web-auth**]

The SNMP agent is forbidden to send Trap messages to the NMS by default.

(5) (Optional) Configure the system reboot trap sending function.

snmp-server system-shutdown

The SNMP system reboot notification function is disabled by default.

(6) (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.

(7) (Optional) Include private fields in sent Trap messages.

snmp-server trap-format private

SNMP Trap messages do not include private fields by default.

(8) 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.

(9) (Optional) Enable the function of carrying the device SN in the Trap message.

snmp-server trap-format device-serial-number

This function is disabled by default.

(10) (Optional) Enable the function of carrying the SYSMAC in the Trap message.

snmp-server trap-format sysmac

This function is disabled by default.

(11) (Optional) Enable the Link Trap message sending function on an interface.

a Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

interface aggregateport *interface-number*

- Enter the SVI configuration mode.

  interface vlan *interface-number*

b 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.

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) Enable the SNMP agent function of a device.

enable service snmp-agent

The SNMP agent function is disabled 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 practice, you can disable unused SNMP versions by running the **no snmp-server enable version** [**v1** | **v2c** | **v3**] command.
- All the parameters are optional. Set them based on requirements.

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.

snmp-server enable version [**v1** | **v2c** | **v3**]

SNMPv1 and SNMPv2c are disabled and SNMPv3 is enabled by default.

(14) Enable sending the heartbeat Trap message.

snmp-server heartbeat on

This function of sending the heartbeat Trap message is enabled by default.

(15) Configure the interval for sending the heartbeat Trap message.

snmp-server heartbeat period *seconds*

The default interval is 300s.

(16) Configure the local engine ID.

snmp-server local-engineid *engineid*

The local engine ID is automatically generated by default. The default length is 11 bytes. The first bit has a fixed binary value of 1, and the first four bytes are the private number of the enterprise device allocated by IANA, which is a fixed decimal value of 4881, so the fixed hexadecimal value of the first five bytes is 8000131103. The last six bytes are the MAC address.

1.7 Monitoring

Run the **show** command to check the configuration.

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

⚠ Caution

During device operation, running the **clear** command may cause service interruption due to key information loss.

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.
clear snmp locked-user	Clears information of users that are locked after SNMP authentication fails consecutively.
clear snmp proc-mib-time-list	Clears the SNMP MIB timer counters.
show snmp [**group** | **host** | **locked-ip** | **locked-user** | **message** | **mib** | **oid |** **process-mib-time** | **trap** | **user** | **version** | **view**]	Displays the SNMP status information.

1.8 Configuration Examples

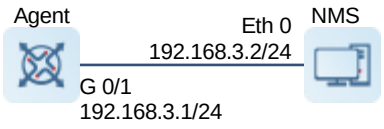
1.8.1 Configuring Basic SNMPv2c Function

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 SNMPv2c Function



3. Procedure

Enable the SNMP agent function.

```
Device> enable
Device# configure terminal
Device(config)# enable service snmp-agent
```

Configure a read/write community with the name community_name.

```
Device(config)# snmp-server community community_name rw
```

Configure an IP address for the agent: set the address of GigabitEthernet 0/1 to 192.168.3.1/24, so that the agent can access the NMS.

```
Device(config)# interface gigabitEthernet 0/1
Device(config-if-gigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Device(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.

```
Device# 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.

```
Device# show service
snmp-agent    : enabled
ssh-server    : disabled
telnet-server : enabled
```

5. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
 ip address 192.168.3.1 255.255.255.0
!
snmp-server community community_name rw
!
end
```

1.8.2 Configuring Basic SNMPv3 Function

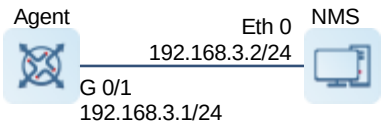
1. Requirements

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 SNMP user group.
- Configure an SNMP user.
- Configure an SNMP host.
- Configure an IP address for the agent.

4. Procedure

Enable the SNMP agent functio

```
Device> enable
Device# configure terminal
Device(config)# enable service snmp-agent
```

Create an SNMP user group with the name **Snmpv3group**, select v3 as the version, and configure an authentication and encryption mode with the security level priv.

```
Device(config)# snmp-server group Snmpv3group v3 priv
```

Note

In actual scenarios, to improve network security, you can configure a MIB view to control the access permissions of MIB objects. The configuration example is as follows:

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.

```
Device(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.

```
Device(config)# snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

Create an SNMP user group with the name **Snmpv3group**, 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.

```
Device(config)# snmp-server group Snmpv3group v3 priv read view1 write view2
```

Configure an SNMP user. Create a user with the name **Snmpv3user** under the group **Snmpv3group**, select v3 as the version, and set the authentication mode to SHA2-256, authentication password to test1@123, encryption mode to AES128, and encryption password to test2@321.

```
Device(config)# snmp-server user Snmpv3user Snmpv3group v3 auth sha2-256 test1@123
priv aes128 test2@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 **Snmpv3user**.

```
Device(config)# snmp-server host 192.168.3.2 traps version 3 priv Snmpv3user
```

Enable the agent to actively send Trap messages to the NMS.

```
Device(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, so that the agent can access the NMS.

```
Device(config)# interface gigabitEthernet 0/1
Device(config-if-gigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0
Device(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.

```
Device# 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.

```
Device# show snmp user
User name: Snmpv3user
Engine ID: 80001311037042d3a3d3ed
storage-type: permanent    active
Security level: auth priv
Auth protocol: SHA2-256
Auth key: db 24 65 26 3b 1e 7d b0 14 10 2c ec be 93 7a 6a a1 c2 33 f5 19 c5 46 0c 29
c8 16 35 a2 1d 04 cf
Priv protocol: AES
Priv key: db 24 65 26 3b 1e 7d b0 14 10 2c ec be 93 7a 6a
Group-name: Snmpv3group
```

Run the **show snmp group** command to display the SNMP group.

```
Device# show snmp group
groupname: Snmpv3group
securityModel: v3
securityLevel:authPriv
readview:
writeview:
notifyview:
```

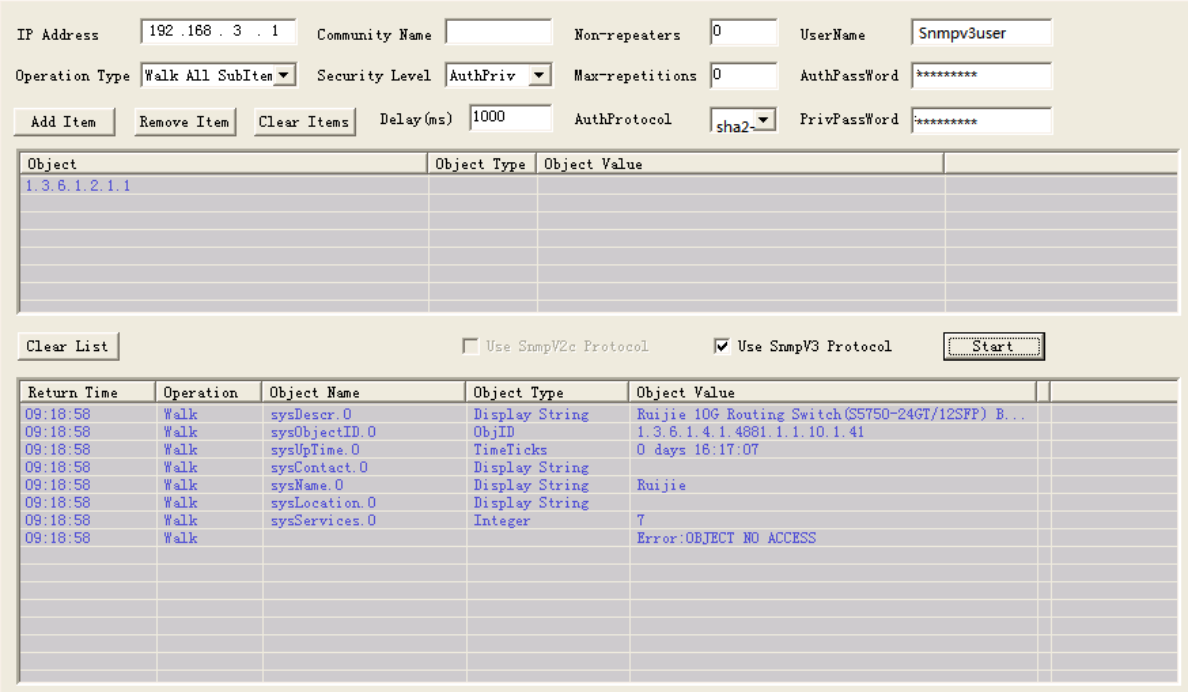
Run the **show snmp host** command to display the host information configured by the user.

```
Device# show snmp host
Notification host: 192.168.3.2
```

```
udp-port: 162
type: trap
user: Snmpv3user
security model: v3 authPriv
```

In the NMS, enter the IP address of the device: 192.168.3.1 and **Snmpv3user** in UserName, select AuthPriv for Security Level, enter **test1@123** in AuthPassWord, select **SHA2-256** for AuthProtocol, and enter **test2@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 192.168.3.1 255.255.255.0
!
snmp-server user Snmpv3user Snmpv3group v3 encrypted auth sha2-256
DB2465263B1E7DB014102CECBE937A6AA1C233F519C5460C29C81635A21D04CF priv aes128
DB2465263B1E7DB014102CECBE937A6A
snmp-server group Snmpv3group v3 priv
snmp-server host 192.168.3.2 traps version 3 priv Snmpv3user
snmp-server enable traps
!
end
```

7. Common Errors

The authentication and encryption modes selected on the network management software are inconsistent with those configured on the device, causing MIB operation failures.

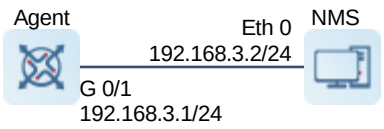
1.8.3 Configuring Basic Trap Function

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: set the IP address of GigabitEthernet 0/1 on the agent to 192.168.3.1.

```
Device> enable
Device# configure terminal
Device(config)#interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Device(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 Snmpv3user. Enable the agent to actively send Trap messages to the NMS.

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 192.168.3.2 traps version 2c Snmpv3user
Device(config)# snmp-server enable traps
```

4. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Device# 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.

```
Device# 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
       33 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
7 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
       7 Trap PDUs
SNMP global trap: enabled
SNMP logging: disabled
SNMP trap logging: disabled
SNMP authentication success logging: enabled
SNMP authentication fail logging: enabled
SNMP agent: enabled
SNMP v1:  enabled
SNMP v2c: enabled
SNMP v3:  enabled
```

5. Configuration Files

Agent configuration file

```
interface GigabitEthernet 0/1
 ip address 192.168.3.1 255.255.255.0
!
snmp-server host 192.168.3.2 traps version 2c Snmpv3user
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 the company's 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 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.

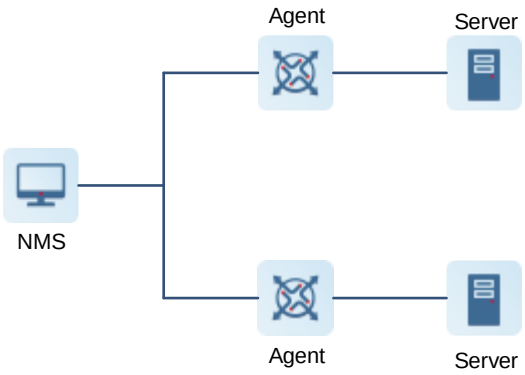
- RMON history statistics function

  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
- RFC 4502: 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) Enter the Layer 2 or Layer 3 Ethernet interface configuration mode.

interface *ethernet-type interface-number*

(4) 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 Layer 2 or Layer 3 Ethernet interface configuration mode.

interface *ethernet-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*.
- 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** *sampling-rising-threshold-value* [*event-number*] **falling-threshold** *falling-threshold-value* [*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 history	Displays the history control table information.
show rmon alarm	Displays the alarm table information.
show rmon event	Displays the event table information.
show rmon sql	Displays RMON database information.
show rmon statistics	Displays Ethernet statistics.
show rmon timer	Displays RMON timer information.

1.7 Configuration Examples

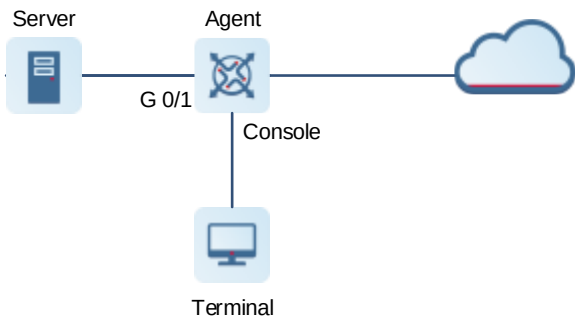
1.7.1 Configuring the Ethernet Statistics Function

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.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin
```

4. Verification

Run the **show rmon stats** command to display Ethernet statistics information.

```
Device# 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 Device
!
interface GigabitEthernet 0/1
 rmon collection stats 1 owner admin
!
end
```

6. Common Errors

The parameters of configured statistics entries are reconfigured or modified.

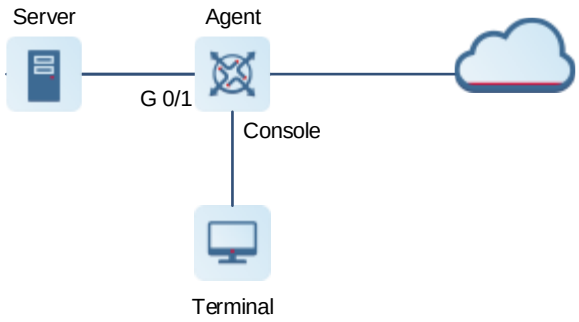
1.7.2 Configuring the History Statistics Function

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.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1
Device(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.

```
Device# 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 Device
!
interface GigabitEthernet 0/1
rmon collection history 1 owner admin buckets 5 interval 300

!
end
```

6. Common Errors

The parameters of configured history control entries are reconfigured or modified.

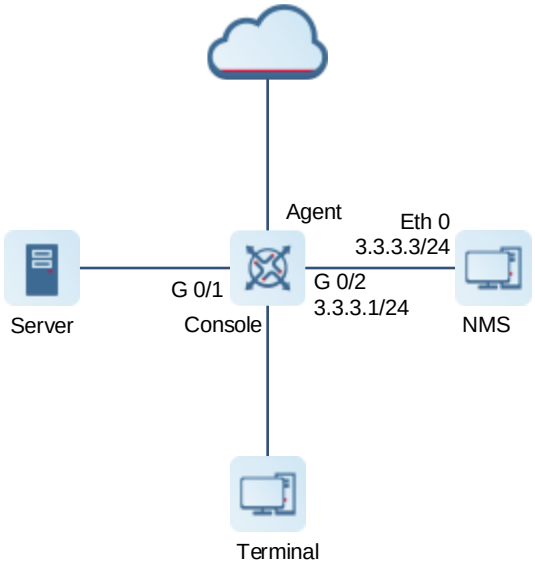
1.7.3 Configuring the Alarm Function

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.

```
Device> enabel
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 3.3.3.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
```

Configure an event group to process alarms.

```
Device(config)# snmp-server community public1 rw
Device(config)# snmp-server host 3.3.3.3 trap public1
Device(config)# rmon event 1 description rising-threshold-event log trap public1 owner
admin
Device(config)# rmon event 2 description falling-threshold-event log owner admin
```

Configure the alarm function.

```
Device(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.

```
Device# 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.

```
Device# 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.

```
Device# 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 Device
!
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 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 5
1.1.5 Protocols and Standards 6
1.2 Configuration Task Summary 7
1.3 Configuring Communication Between the NETCONF Server and Client 7
1.3.1 Overview 7
1.3.2 Restrictions and Guidelines 7
1.3.3 Prerequisites 8
1.3.4 Procedure 8
1.4 Configuring NETCONF Authentication 9
1.4.1 Overview 9
1.4.2 Restrictions and Guidelines 9
1.4.3 Procedure 9
1.5 Monitoring 10
1.6 Configuration Examples 11
1.6.1 Configuring NETCONF 11
1.6.2 Configuring NETCONF Authentication 15

1 Configuring NETCONF

1.1 Introduction

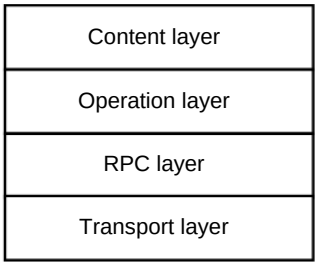
1.1.1 Overview

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 client runs the client program 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. The client uses the <rpc> element to encapsulate the NETCONF request message, and the server uses the <rpc-reply> element to encapsulate the NETCONF reply message. 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

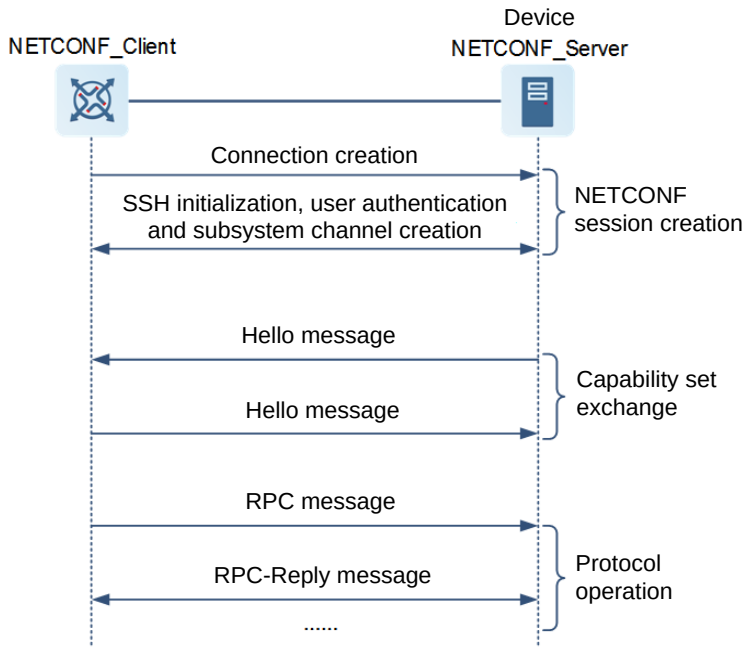
4. Content Layer

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

The 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 client 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.
- Get-config: Obtains configuration data based on the filtering node.

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.
- Delete: Deletes configuration data that includes this attribute in the Edit-config packets from the specified configuration file or database.
- Remove: Removes configuration data that includes this attribute in the Edit-config packets from the specified configuration file or database.

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.
- Delete-config: Deletes the configuration file. It is not allowed to delete the running file.

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).

Note

According to RFC 6241, 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 removes some functions of the 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.
- Close-session: Closes the current session, including resource and lock release and disconnection.

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 clients and the access to NETCONF resources, allowing the clients 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, authorized clients 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

RPC Method	Function	Default Permission (R: read; W: write; X: execute)
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
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

- RFC 4741: NETCONF Configuration Protocol

- RFC 4742: Using the NETCONF Configuration Protocol over Secure Shell (SSH)
- RFC 4743: Using NETCONF over the Simple Object Access Protocol (SOAP)
- RFC 4744: Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)
- RFC 5277: NETCONF Event Notifications
- RFC 5381: Experience of Implementing NETCONF over SOAP
- RFC 5539: NETCONF Over Transport Layer Security (TLS)
- RFC 5717: Partial Lock RPC for NETCONF
- RFC 6022: NETCONF Monitoring Schema
- RFC 6241: Network Configuration Protocol
- RFC 6242: Using the Network Configuration Protocol over Secure Shell
- RFC 6243: With-defaults capability for NETCONF
- RFC 6470: NETCONF Notification Events
- RFC 6536: NETCONF Access Control Model (NACM)

Note

RFC 4741 and RFC 4742 have been replaced by RFC 6241 and RFC 6242 respectively.

1.2 Configuration Task Summary

NETCONF configuration includes the following tasks:

(1) Configuring Communication Between the NETCONF Server and Client

(2) (Optional) Configuring NETCONF Authentication

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 Configuring NETCONF Authentication

1.4.1 Overview

The NETCONF authentication mechanism is configured to manage the NETCONF operations of specific clients and the access to NETCONF resources, allowing the clients to perform operations and access data nodes stipulated by NETCONF.

1.4.2 Restrictions and Guidelines

- A user group cannot be named with the asterisk (*), because the symbol indicates all user groups.
- For a single rule list, the rules are successively matched based on the rule configured by users. When an operation matches a permit rule, the operation is permitted. When an operation matches a deny rule or does not match a rule, the operation is denied in the current rule list.
- For multiple rule lists, the rules in the lists are matched based on the rule configuration sequence. When an operation matches a permit rule in a rule list, the operation is permitted. When an operation matches a deny rule, the operation is denied. When an operation does not match any rule in the list, the operation matches the rules of the next list.
- RPC operation methods include Get, Get-Config, Edit-Config, Copy-Config, Delete-Config, Validate, Commit, Cancel-Commit, Discard-Changes, Lock, Kill-Session, and Get-Schema.
- If no rule type is configured, permission control is applied to both RPC operation methods and data node rules.
- Rule control for enabling RPC operation methods can be configured. If the Execute permission is included in the access operation permissions configured under the rules, the rules are matched during RPC operation method check. Otherwise, such rule matching does not occur.
- Rule control for enabling data nodes can be configured. If at least one of the Create, Read, Update and Delete permissions is included in the access operation permissions configured under the rules, the rules are matched during data node check. Otherwise, such rule matching does not occur.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the authentication configuration mode.

netconf acm

(4) Configure a user group and enter the authentication user group configuration mode.

user-group-name *name*

No user group is configured by default.

(5) Associate users with the user group.

user-name *name*

No user is associated with a user group by default.

(6) Quit the authentication configuration mode.

exit

(7) Configure a rule list and enter the authentication rule list configuration mode.

rule-list *name*

No rule list is configured by default.

(8) Associate the user group with the rule list.

user-group { ***** | *name* }

No user group is associated with a rule list by default.

(9) Configure rules and enter the rule mode of the authentication rule list.

rule *name* **action** { **permit** | **deny** }

No rule is configured by default.

(10) Configure rule types.

rule-type { **rpc-name** { *name* | ***** } | **path** *path* }

No rule type is configured by default.

(11) Configure access permissions of the rules.

access-operation { * | { create | delete | exec | read | update } * }

No access permission of a rule is configured by default.

1.5 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 candidate-tree	Displays the configuration received by the NETCONF candidate database.
show netconf capability	Displays information about NETCONF capabilities.
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 schema-node-path [*module*]	Displays the YANG path corresponding to the YANG model.
show netconf yang tree	Displays all YANG model trees supported currently.

1.6 Configuration Examples

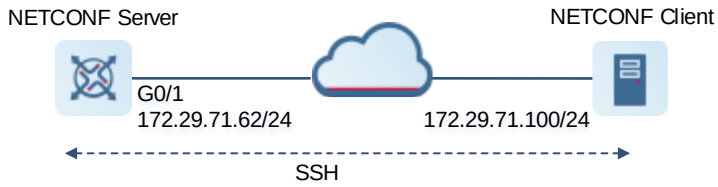
1.6.1 Configuring NETCONF

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 gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1))# ip address 172.29.71.62 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1))# exit
```

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 net_1234.

```
Hostname(config)# username netconf privilege 15 password net_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.

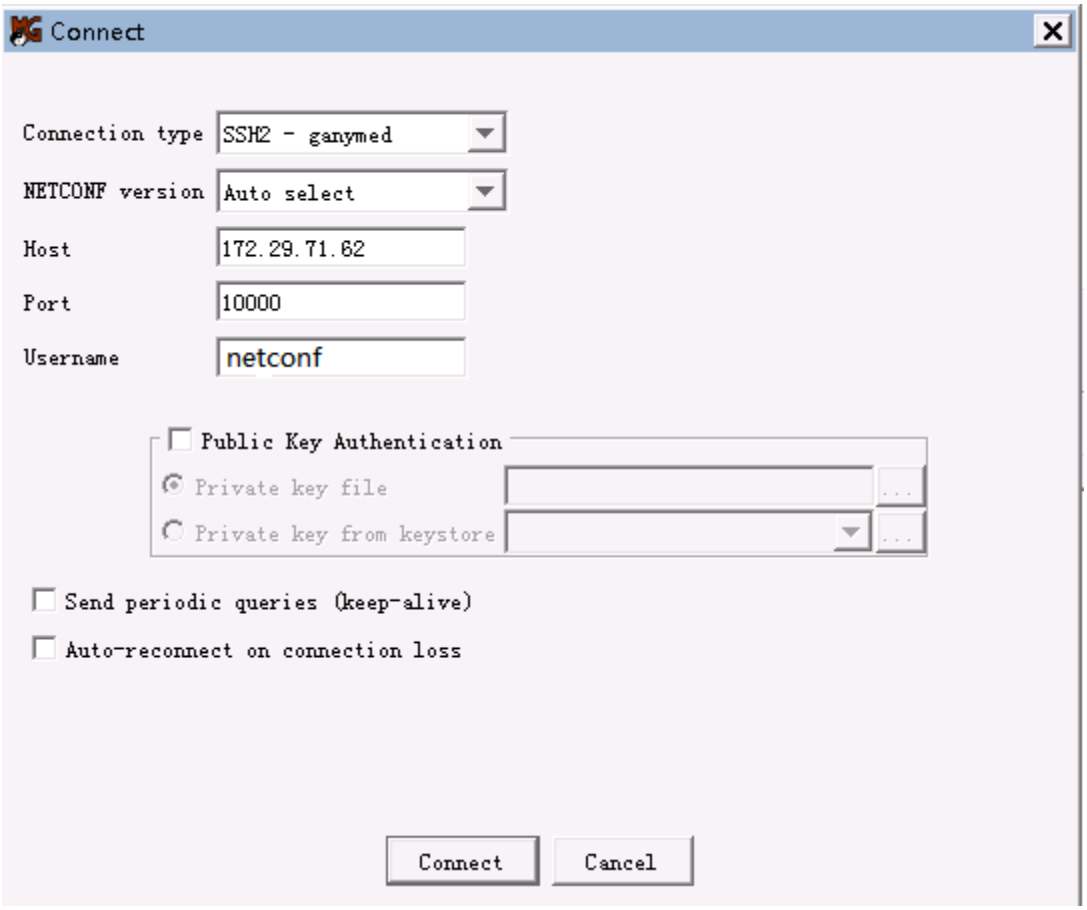
```
Hostname(config)# netconf log session
```

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 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 kill session    : 0
Session unsupport      : 0
Session lock_or_unlock  : 0
======================================================================
```

6. Configuration Files

- NETCONF_Server configuration file

```
hostname Hostname
!
username netconf privilege 15 password 7 $10$393$wpgQ1hbo7hc=$
!
netconf log session
netconf capability candidate
netconf port 5000
netconf max-sessions 6
netconf timeout 100
!
enable service ssh-server
!
interface GigabitEthernet 0/1
 ip address 172.29.71.62 255.255.255.0
!
line vty 0 35
 login local
!
end
```

1.6.2 Configuring NETCONF Authentication

1. Requirements

The user **user1** has the permission to get all modules, and the user **user2** has the permission to create SNMP modules.

2. Topology

Figure 1-5 Topology of NETCONF Authentication

3. Notes

Configure the Get permission for all modules for **user1**.

Configure the Create permission for SNMP modules for **user2**.

4. Procedure

(1) Configure the Get permission for all modules for **user1**.

Configure a user **user1**.

```
Device> enable
Device# configure terminal
Device(config)# username user1 password test_12345
```

Enter the authentication configuration mode.

```
Device(config)# netconf acm
```

Configure a user group **guser1**.

```
Device(config-nacm)# user-group-name guser1
```

Associate **user1** with **guser1**.

```
Device(config-nacm-user-group)# user-name user1
Device(config-nacm-user-group)# exit
```

Configure a rule list rule-list1.

```
Device(config-nacm)# rule-list rule-list1
```

Associate **guser1** with rule-list1.

```
Device(config-nacm-rule-list)# user-group guser1
```

Configure a permit rule rule1.

```
Device(config-nacm-rule-list)# rule rule1 action permit
```

Configure the RPC method as Get.

```
Device(config-nacm-rule-list-rule)# rule-type rpc-name get
Device(config-nacm-rule-list-rule)# end
```

(2) Configure the Create permission for SNMP modules for **user2**.

Configure a user **user2**.

```
Device# configure terminal
Device(config)# username user2 password test_12345
```

Enter the authentication configuration mode.

```
Device(config)# netconf acm
```

Configure a user group **guser2**.

```
Device(config-nacm)# user-group-name guser2
```

Associate a user group **user2** with a user **guser2**.

```
Device(config-nacm-user-group)# user-name user2
```

Configure a rule list rule-list2.

```
Device(config-nacm-user-group)# exit
```

Associate a user group **guser2** with a rule list rule-list2.

```
Device(config-nacm)# rule-list rule-list2
Device(config-nacm-rule-list)# user-group guser2
```

Configure a permit rule rule2.

```
Device(config-nacm-rule-list)# rule rule2 action permit
```

Configure a data node type and configure the data node as an SNMP module name.

```
Device(config-nacm-rule-list-rule)# rule-type path /rg-snmp:snmp
```

Configure the access permission as Create.

```
Device(config-nacm-rule-list-rule)# access-operation create
```

5. Verification

Run the **show netconf authorization user-name user1 user-group** command to display user group information of a user **user1**.

```
Device # show netconf authorization user-name user1 user-group
UserGroup: guser1
```

Run the **show netconf authorization user-name user2 user-group** command to display user group information of a user **user2**.

```
Device # show netconf authorization user-name user2 user-group
UserGroup: guser2
```

Run the **show netconf authorization user-name user1 rule-list detail** command to display details of the rule list associated with a user **user1**.

```
Device# show netconf authorization user-name user1 rule-list detail
RuleList: rule-list1
  ---------------------------------------------------------------------
  Rule           Action   AccessOperation   Type     Entity
  ---------------------------------------------------------------------
  rule1          permit   RCUDX           RPC      get
  [R:Read C:Create U:Update D:Delete X:Exec]
```

Run the **show netconf authorization user-name user2 rule-list detail** command to display details of the rule list associated with a user **user2**.

```
Device# show netconf authorization user-name user2 rule-list detail
RuleList: rule-list2
  ------------------------------------------------------------------
  Rule           Action   AccessOperation   Type     Entity
  ------------------------------------------------------------------
  rule2          permit   -C---           PATH     /rg-snmp:snmp
  [R:Read C:Create U:Update D:Delete X:Exec]
```

6. Configuration Files

Device configuration file

```
hostname Device
!
username user1 password 7 $10$391$/9kemZ1jG1+E0A==$
username user2 password 7 $10$0cb$3opZPP7Q4HmK9g==$
!
netconf acm
 user-group-name guser1
  user-name user1
 user-group-name guser2
  user-name user2
 rule-list rule-list1
  user-group guser1
  rule rule1 action permit
   rule-type rpc-name get
 rule-list rule-list2
  user-group guser2
  rule rule2 action permit
   access-operation create
   rule-type path /rg-snmp:snmp
!
end
```

Contents

1 Configuring gRPC 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 gRPC 5
1.3.1 Overview 5
1.3.2 Restrictions and Guidelines 5
1.3.3 Procedure 5
1.4 Configuring the gRPC Response Timeout Time 5
1.4.1 Overview 5
1.4.2 Restrictions and Guidelines 5
1.4.3 Procedure 5
1.5 Configuring Event Types Supported by gRPC 6
1.5.1 Overview 6
1.5.2 Restrictions and Guidelines 6
1.5.3 Procedure 6
1.6 Configuring gRPC to Support Pre-configuration Functions 7
1.6.1 Configuration Tasks 7
1.6.2 Configuring gRPC to Pre-configure a Subscription Server and Event 7
1.6.3 Configuring gRPC to Support User Login Information of the Functional Server 8
1.7 Configuring a YANG Model Path 9

1.7.1 Overview 9
1.7.2 Restrictions and Guidelines 9
1.7.3 Procedure 9
1.8 Configuring the gRPC Subscription Function 9
1.8.1 Overview 9
1.8.2 Restrictions and Guidelines 9
1.8.3 Configuration Tasks 10
1.8.4 Configuring gRPC to Specifying a Source Interface to Send Data 10
1.8.5 Configuring gRPC Destination Server 10
1.8.6 Configuring gRPC Subscription 11
1.9 Configuring gRPC to Support the Login and Logout Function 12
1.9.1 Overview 12
1.9.2 Restrictions and Guidelines 12
1.9.3 Procedure 12
1.10 Configuring a Third-party Defined RPC Method 12
1.10.1 Overview 12
1.10.2 Procedure 13
1.11 Configuring a Dial-out RPC Method 13
1.11.1 Overview 13
1.11.2 Procedure 13
1.12 Configuring gRPC Server 13
1.12.1 Overview 13
1.12.2 Configuration Tasks 13
1.12.3 Enabling gRPC Server 14

1.12.4 Configuring gRPC Server Port Number....14
1.12.5 Configuring the Source Port Bound to gRPC Server....14
1.12.6 Loading the SSL/TLS Certificate....15
1.12.7 Loading the CA Certificate....15
1.12.8 Configuring ACL Filter Rule....16
1.12.9 Configuring IP Blocking for the gRPC Server....16
1.13 Monitoring....17
1.14 Configuration Examples....18
1.14.1 Configuring Basic Functions of gRPC....18

1 Configuring gRPC

1.1 Introduction

1.1.1 Overview

The Google Remote Procedure Calls (gRPC) is a high-performance open source software framework developed by Google using the Hyper Text Transfer Protocol 2 (HTTP2) as a data transmission protocol. gRPC provides a network configuration and management method that supports multiple programming languages. On the gRPC framework, secondary development can be performed.

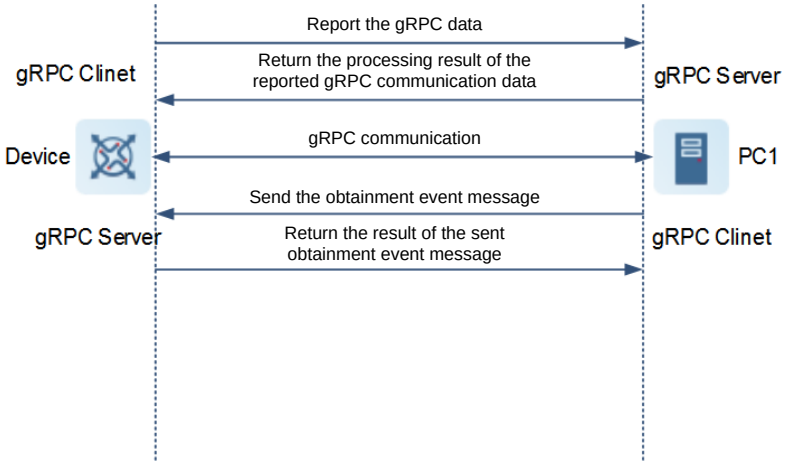
1.1.2 Principles

1. Enabling the gRPC Function

After gRPC is enabled on the device, the device can function as a gRPC Server to receive authentication requests and obtain messages and as a gRPC Client to report gRPC data.

gRPC communication is implemented over the HTTP2 protocol. After a gRPC client initiates a request and a server returns a response, a data interaction is completed. Only the client can initiate a request, and the end of the interaction is indicated by the receipt of a response from the server. See Figure 1-1.

Figure 1-1 gRPC Communication Flow



(1) After gRPC is configured on the device, the gRPC Client and gRPC Server services are enabled.

(2) The gRPC Server of the device receives an obtainment event message from the server, and returns a response to the obtainment event to the server.

(3) The gRPC Client of the device reports gRPC data to the gRPC Server of the server based on the subscribed event type and waits for a response.

2. Supporting Login and Logout Functions

- Supporting Login Initiated by the Server

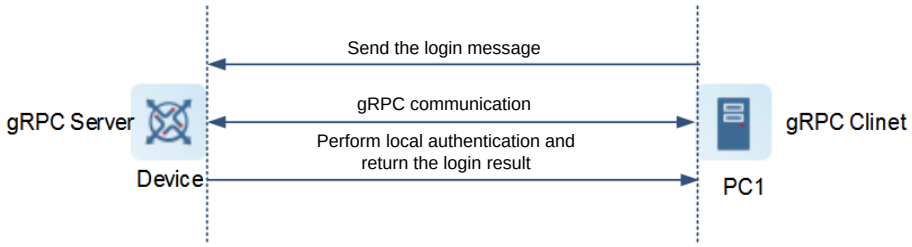
a After gRPC is configured on the device, the gRPC Server services are enabled.

b The device receives a login request initiated by the server, authenticates the server locally, and returns a login result to the server.

c The gRPC Server of the device receives only the obtainment events initiated by the server that has been logged in.

For the procedure, see Figure 1-2.

Figure 1-2 gRPC Login Flow



- Supporting Logout Initiated by the Server

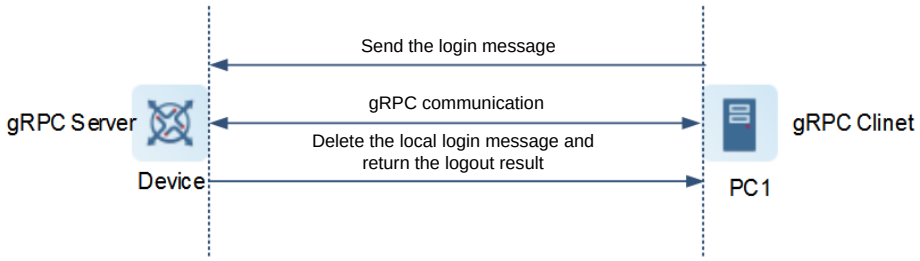
a After gRPC is configured on the device, the gRPC Server services are enabled.

b The device receives a logout request initiated by the server, deletes the local matched login information, and returns a logout result to the server.

c The gRPC Server of the device does not receive the obtainment events initiated by the server that has been logged out.

For the procedure, see Figure 1-3.

Figure 1-3 gRPC Logout Flow



3. Supporting Some Event Types

gRPC supports realtime events, periodic events, and obtainment events.

- Realtime events: This type of events are triggered when a specified threshold is met, irrespective of time. In this case, the device collects information once and reports it to the server.
- Periodic events: This type of events are reported regularly. When the time is up, the device collects information once and reports it to the server.
- Obtainment events: This type of events are initiated by the server to query data. After the device receives a query request, the device collects information and reports it to the server.

4. Supporting Server Subscription and Events

The device can pre-create a server to be subscribed to and an event of concern based on a configured command or NETCONF or other channels.

The device can configure a standby server based on a configured command or NETCONF or other channels. When the active server becomes faulty, it automatically sends data to the standby server.

The device can delete the subscription server and event based on a configured command or NETCONF or other channels.

5. Specifying a Source Interface to Send Data

gRPC is configured on the device and a channel is created. Before sending some packets to the server, the device creates a socket and attempts to send ping packets to check whether the path is reachable. If so, the device sends the gRPC packets. By default, the created socket is bound randomly to the source address of a device port to send ping packets. If the server receives only packets from the specified source address, the default behavior of gRPC does not make the path reachable. As a result, gRPC packets cannot be uploaded. If a specified source address is bound when a socket is created, the reachable path can ensure that gRPC packets are correctly uploaded.

6. Supporting User Login Information of the Server

- The device can pre-create a server to be subscribed to and an event of concern based on a configured command or NETCONF or other channels.
- The device can configure a standby server based on a configured command or NETCONF or other channels. When the active server becomes faulty, it automatically sends data to the standby server.
- The device can delete the subscription server and event based on a configured command or NETCONF or other channels.

7. Supporting Data Subscription of the YANG Model

- The device can deliver configuration defined by openconfig-telemetry.yang to collect YANG model data of the device based on a configured command or NETCONF or other channels.
- The device can delete the configuration defined by openconfig-telemetry.yang based on a configured command or NETCONF or other channels.

8. Supporting Third-party Defined RPC Methods

- Running a configured command, the device can enable RPC methods that support the gnmi.proto definition. Data can be collected with the RPC methods such as Get, Set, and Subscribe.
- Running a configured command, the device can disable RPC methods that do not support the gnmi.proto definition.
- Running a configured command, the device can enable RPC methods that support the t_agent.proto and t_health_check.proto definition of openR. openR related functions can be performed with these RPC methods.
- Running a configured command, the device can disable RPC methods that are not defined by openR.

9. Supporting Dial-out RPC Methods

- The device can select an RPC method corresponding to dial-out based on a configured command.

- The device supports gRPC Network Management Interface (gNMI) based open source RPC methods of Sonic.
- The device supports gNMI based private RPC methods.
- The device supports private RPC methods.

- The device can restore the default RPC method based on a configured command. The gNMI based open source RPC methods of Sonic are used by default.

1.2 Configuration Task Summary

gRPC configuration includes the following tasks:

(1) Configuring Basic Functions of gRPC

(2) Configuring the gRPC Response Timeout Time

(3) Configuring Event Types Supported by gRPC

(4) Configuring gRPC to Support Pre-configuration Functions

- Configuring gRPC to Pre-configure a Subscription Server and Event
- Configuring gRPC to Support User Login Information of the Functional Server

(5) Configuring a YANG Model Path

(6) Configuring the gRPC Subscription Function

- (Optional) Configuring gRPC to Specifying a Source Interface to Send Data
- Configuring gRPC Destination Server
-
- Configuring gRPC Subscription

(7) (Optional) Configuring gRPC to Support the Login and Logout Function

(8) Configuring a Third-party Defined RPC Method

(9) Configuring a Dial-out RPC Method

(10) (Optional) Configuring gRPC Server

- Enabling gRPC Server
- Configuring gRPC Server Port Number
- Configuring the Source Port Bound to gRPC Server
- Loading the SSL/TLS Certificate
- Loading the CA Certificate
- Configuring ACL Filter Rule
- Configuring IP Blocking for the gRPC Server

1.3 Configuring Basic Functions of gRPC

1.3.1 Overview

The gRPC function is enabled, and the gRPC Client and gRPC Server are created. The gRPC Client uploads data to the server, and the gRPC Server parses authentication messages sent from the server and obtains the message content.

1.3.2 Restrictions and Guidelines

- The connection between the device and server must be normal.
- The port number of the local gRPC Server is 50051.
- A gRPC instance is created by running a **gRPC** command, the gRPC function is enabled, and the gRPC configuration mode is enabled.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the gRPC function.

grpc

The gRPC function is disabled by default.

1.4 Configuring the gRPC Response Timeout Time

1.4.1 Overview

The data response timeout time is configured for the gRPC Server.

1.4.2 Restrictions and Guidelines

- After the data response timeout time is configured for the gRPC process and the collector delivers a Get or Set operation, a timeout message is returned if the server does not obtain corresponding data within the timeout time.
- The value of the timeout time should be configured based on the actual scenario. If the configured timeout time is too short, part of the required data may not be returned in the timeout period during a Get operation.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure the gRPC data response timeout time.

reply-timeout *time*

The default data authentication timeout time on the gRPC Server is **10** seconds.

1.5 Configuring Event Types Supported by gRPC

1.5.1 Overview

- The device is configured with all realtime events of concern which are subscribed to.
- The device is configured with all periodic events of concern which are subscribed to.
- The timer time of the periodic events is modified.

1.5.2 Restrictions and Guidelines

- The event which the server subscribes to cannot effect unless a specified event which is subscribed to is configured on the device.
- If the device subscribes to a realtime event, a realtime packet is generated and sent to the subscribing server when the threshold of the realtime events is triggered. If the threshold of the realtime events is triggered frequently, many same packets are generated within a short time and sent to the subscribing server. As a result, the cost of the server and the device is added. To prevent such threshold from being triggered frequently, Run the **subscr-realtime-interval** command to suppress realtime events to generate new packets within a period.
- When any periodic events of concern which are subscribed to is configured and the NETCONF manager sends periodic events which are subscribed to, the corresponding periodic timer starts and gRPC data is sent to the subscribing server.
  - If the NETCONF manager does not subscribe to any periodic time, the timer period is determined by the **subscr-sample-interval** command.
  - If the NETCONF manager subscribes to both the periodic events and period time, the period time is subject to the subscription time of the NETCONF manager.
- After any events of concern which are subscribed to are configured by the gRPC process, the gRPC process waits for the NETCONF manager to send the subscription events:
  - If the received subscription message matches the local subscription event, the event triggering gRPC reporting server function is enabled.
  - When the NETCONF manager sends an unsubscription event and the received unsubscription message matches the local subscription event, the event triggering gRPC reporting server function is disabled.
- If no events of concerns which are subscribed to are configured by the gRPC process, the gRPC process ignores the subscription events and unsubscription events sent by the NETCONF manager.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure an event of concern which is subscribed to on the device.

subscr [**realtime** | **sample**] **enable**

No events of concern which are subscribed to are configured by default.

(5) (Optional) Configure the timer time of the periodic events.

subscr-sample-interval *subscr-sample-interval-second* [**millisecond** *subscr-sample-interval-millisecond*]

The default periodic event timer time is **10** seconds.

(6) (Optional) Configure the realtime event suppression time.

subscr-realtime-interval { **all** *subscr-realtime-time* | **realtime** *json-event subscr-realtime-time* }

The realtime event suppression function is not enabled by default.

1.6 Configuring gRPC to Support Pre-configuration Functions

1.6.1 Configuration Tasks

gRPC configuration includes the following tasks:

- Configuring gRPC to Pre-configure a Subscription Server and Event
- Configuring gRPC to Support User Login Information of the Functional Server

1.6.2 Configuring gRPC to Pre-configure a Subscription Server and Event

1. Overview

- After a server and event which are subscribed to is pre-configured, gRPC packets of corresponding events can be reported to the server.
- After a subscribing standby server is pre-configured, its services can be switched over to the standby server and packets are automatically sent to the standby server when the active server becomes faulty.

2. Restrictions and Guidelines

- The address and port number of the subscribing server must be legitimate.
- The events and parameters which are subscribed to must be correct and valid.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure gRPC to support a subscribing server.

user-server *ipv4-address port-number*

No subscribing server is pre-configured by default.

(5) Configure gRPC to support a subscription event.

type *json-event* **value** *value-interval* [**value-extend** *value-extend-interval*]

The event subscription function for a specified server is not enabled by default.

(6) (Optional) Configure gRPC to support the heartbeat detection function.

heartbeat inform [**interval** *interval*] [**keepalive-times** *keepalive-times*]

The heartbeat sending function is not enabled by default.

(7) (Optional) Configure gRPC to pre-configure a standby server for the subscribing server.

standby-server *ipv4-address port-number*

No standby server is pre-configured for the subscribing server by default.

Before configuring a standby server, enable the heartbeat detection function. When an active server becomes faulty, data can be automatically sent to the standby server.

(8) (Optional) Exit the gRPC subscription server configuration mode.

exit-user-server

1.6.3 Configuring gRPC to Support User Login Information of the Functional Server

1. Overview

After user login information is pre-configured for the server, the specified server can obtain correct information after initiating an obtainment event request.

2. Restrictions and Guidelines

- Running a configured command, the device can pre-create user login information of the server that passes authentication, simulate the server to initiate a login request, pass the authentication, and save the user login information.
- Running a configured command, the device can delete user login information of the server that passes authentication, simulate the server to initiate a logout request, and delete the user login information.
- The address of the server must be legitimate.
- The sequence number of the login user must be unique.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure gRPC to pre-configure user login information of the server.

user-client *user-id username ipv4-address*

No user login information is pre-configured for the server by default.

1.7 Configuring a YANG Model Path

1.7.1 Overview

After the YANG model path and data source are collected, data can be sent to the corresponding server based on the path in the subscription association relationship.

1.7.2 Restrictions and Guidelines

- The YANG model path must be legitimate and corresponding data is available on the path.
- In the YANG model path group, a specific YANG model path is configured. For the detailed compilation method of the path, see the displayed information of the **show grpc yang tree** and **show grpcnode-path** commands in **gRPC Command Reference**.
- After a gRPC YANG model path group is configured, the system switches to the gRPC YANG model path group configuration mode.
- Multiple YANG model paths can be configured for this group in this mode.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure a YANG model path group, and enter the gRPC YANG model path group configuration mode.

sensor-group *sensor-group-id*

No YANG model path group is configured by default.

(5) Configure a gRPC YANG model path and its group.

sensor-**path** *sensor-path*

No YANG model path is configured by default.

1.8 Configuring the gRPC Subscription Function

1.8.1 Overview

After a subscription association relationship is configured, data of the associated YANG model path group is collected and sent to the destination server of the associated destination group.

1.8.2 Restrictions and Guidelines

A YANG model path group must be configured in advance.

1.8.3 Configuration Tasks

gRPC subscription configuration includes the following tasks:

(1) (Optional) Configuring gRPC to Specifying a Source Interface to Send Data

(2) Configuring gRPC Destination Server

(3) Configuring gRPC Subscription

1.8.4 Configuring gRPC to Specifying a Source Interface to Send Data

1. Overview

gRPC is configured to send packets based on the IP address of a specified interface.

2. Restrictions and Guidelines

- The bound interface must be up and be configured with an IP address.
- If a server receives only packets from a specified source address, this command can be used to configure the specified source interface.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) (Optional) Configure a source interface of realtime data and periodic data.

subscr-source-interface *interface-type interface-number*

The source interface of realtime data and periodic data is a random value by default.

1.8.5 Configuring gRPC Destination Server

1. Overview

The address of a destination server is configured for the server to subscribe to a YANG model path in the subscription association relationship.

2. Restrictions and Guidelines

- The address and port number of the server must be legitimate.
- After a gRPC destination group is configured, the system switches to the gRPC destination group configuration mode.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure a gRPC destination group, and enter the gRPC destination group configuration mode.

destination-group *destination-group-id*

No destination group is configured for the subscription association relationship by default.

(5) Configure a gRPC destination address.

- Configure an IPv4 destination address.

  ip *ipv4-address* **port** *port-number*

  No IPv4 address or port is configured for the destination server by default.

- Configure an IPv6 destination address.

  ipv6 *ipv6-address* **port** *port-number*

  No IPv6 address or port is configured for the destination server by default.

(6) Configure a protocol for the destination server.

protocol grpc { **tls** | **no-tls** }

The default protocol is the gRPC protocol that supports plain text transmission.

1.8.6 Configuring gRPC Subscription

1. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure a subscription association relationship group, and enter the gRPC subscription association relationship configuration mode.

subscription *subscriptionid*

No subscription association relationship is configured between the YANG model path group and destination group by default.

(5) Configure the associated YANG model path group and its period interval.

sensor-group *sensor-group-id* [**sample-interval** *sample-interval*]

(6) Configure a destination group of the subscription association relationship.

destination-**group** *destination-group-id*

No destination group is configured for the subscription association relationship by default.

(7) (Optional) Configure a data encoding format.

encoding { **json** | **json-ietf** }

gRPC uses the JavaScript Object Notation (JSON) encoding format by default.

1.9 Configuring gRPC to Support the Login and Logout Function

1.9.1 Overview

The authentication mode of the gRPC login and logout function is configured as authentication-exemption, AAA local authentication, or AAA server authentication (timeout time and retry times are configurable).

1.9.2 Restrictions and Guidelines

- If the authentication mode is configured as AAA server authentication, the new-model must be enabled.
- The authentication-exemption mode is not recommended.
- You are not advised to modify the timeout time and retry times. During server login in the AAA server authentication mode, if the retry times exceed a limit or the timeout time is too long, AAA may be locked for 15 minutes. The lock time can be canceled by running the AAA command **clear aaa local user lockout all**.
- Upon receiving a login request from the server, the device selects one of the three modes based on the configured authentication mode. After the server passes the authentication, the user login information, namely, IP address and username of the server, is recorded. The device returns responses to the obtainment event requests of the server that passes the authentication.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure an authentication mode of the gRPC login and logout function.

authen login { **local** | **authentication** *mlist* }

The local authentication mode, namely, **authen login local** is used by default.

(5) (Optional) Configure the AAA server authentication attribute of the gRPC login and logout function.

authen aaa-config { **retry** *retry-times* | **timeout** *timeout-time* }

The retry times and timeout time of AAA server authentication are 1 and 4 seconds, respectively, by default.

This authentication mode can be configured only after AAA configuration (aaa new-model) is completed.

1.10 Configuring a Third-party Defined RPC Method

1.10.1 Overview

After a third-party defined RPC method is configured, the RPC method can be used to collect device information and data or perform RPC-related operation.

1.10.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure a third-party defined RPC method.

rpc { **gnmi** | **openr** } **enable**

No RPC defined by gNMI or openR is configured by default.

1.11 Configuring a Dial-out RPC Method

1.11.1 Overview

An RPC method is configured for dial-out so that the RPC method can be selected to receive and send messages.

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Configure a dial-out RPC method.

dial-out rpc { **sonic** | **custom** }

The RPC method defined by the open source of Sonic is used by default.

1.12 Configuring gRPC Server

1.12.1 Overview

When you need to use gRPC as the server, you can configure the gRPC server functions.

1.12.2 Configuration Tasks

The configuration tasks of the gRPC Server include:

(1) Enabling gRPC Server

(2) Configuring gRPC Server Port Number

(3) Configuring the Source Port Bound to gRPC Server

(4) Loading the SSL/TLS Certificate

(5) Loading the CA Certificate

(6) Configuring ACL Filter Rule

(7) Configuring IP Blocking for the gRPC Server

1.12.3 Enabling gRPC Server

1. Overview

If you only need to use the dial-out mode after the gRPC function is enabled, you do not need to enable the gRPC server function. You can disable the gRPC server function by using command.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) Enable the gRPC server function.

server enable

By default, the gRPC server is disabled. If you enable the gRPC function, the gRPC server is also enabled.

1.12.4 Configuring gRPC Server Port Number

1. Overview

Modifying the private port number of the server can reduce the probability of scanning attacks.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) (Optional) Configure the gRPC server port number.

server port *port*

By default, the listening port number of the gRPC server is 50051.

1.12.5 Configuring the Source Port Bound to gRPC Server

1. Overview

After you bind the source interface, gRPC clients can only access the gRPC server through the IP address of the interface, improving the access security.

2. Restrictions and Guidelines

- If there are multiple IPv6 addresses on the source interface, the gRPC server supports only the first IPv6 address, and does not support IPv6 link-local addresses or IPv4-mapped IPv6 addresses.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) (Optional) Configure the source interface bound to the gRPC server.

server source-interface *interface-type interface-number*

By default, the source interface bound to the gRPC server is not configured.

1.12.6 Loading the SSL/TLS Certificate

1. Overview

The SSL/TLS certificate can implement TLS encryption.

2. Restrictions and Guidelines

- Before loading the SSL/TLS certificate, you need to copy the certificate to the Flash memory partition of the device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) (Optional) Load the SSL/TLS certificate of the gRPC server.

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

By default, no SSL/TLS certificate is loaded.

1.12.7 Loading the CA Certificate

1. Overview

The CA certificate can be used to perform authentication for clients.

2. Restrictions and Guidelines

- Before loading the CA certificate, you need to copy the certificate to the Flash memory partition of the device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) (Optional) Load the trusted CA certificate for gRPC server.

server trusted-ca load *cert-filename*

By default, no CA certificate is loaded.

1.12.8 Configuring ACL Filter Rule

1. Overview

When you need to filter the illegal connections of the client, you can configure the ACL filter rules of the gRPC server.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the gRPC configuration mode.

grpc

(4) (Optional) Configure the ACL filter rule for gRPC server.

server access-class { **ipv4** { *acl-name* | *acl-number* } | **ipv6** *acl-name* }

By default, no ACL filter rule is configured.

1.12.9 Configuring IP Blocking for the gRPC Server

1. Overview

With IP blocking configured, when the number of authentication failures from a gRPC client reaches the threshold for IP blocking, the IP blocking mechanism is triggered, that is, the gRPC client with this source IP address is not allowed to log in, thereby preventing malicious attacks. After the blocking interval expires, the gRPC client with the IP address is allowed to log in again. 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) Enter the gRPC configuration mode.

grpc

(4) Enable IP blocking for the gRPC server.

ip-block disable

IP blocking is enabled for the gRPC server by default.

(5) (Optional) Configure the maximum number of authentication failures and the interval for counting the number of authentication failures for IP blocking.

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

By default, the maximum number of authentication failures is 6, and the number of authentication failures is counted at an interval of 5 minutes.

(6) (Optional) Configure the IP blocking interval for the gRPC server.

ip-block reactive *reactive-interval*

The default IP blocking interval for the gRPC server is 5 minutes. After the IP blocking interval expires, the gRPC client with the IP address is allowed to log in again.

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 **Bold** commands may lose vital information and thus interrupt services.

Table 1-1 gRPC Monitoring

Command	Purpose
clear grpc channel [*ipv4-address port-number*] [**counter**]	Clears statistics about the server which gRPC subscribes to.
clear grpc subscr [**sample**] [**counter**]	Clears data about periodic events and realtime events of gRPC.
show grpc channel [**counter**]	Displays server address, port number, subscription events, and different statistics.
show grpc client	Displays gRPC server login information.
show grpc status	Displays gRPC running status information.
show grpc subscr [**realtime** | **sample**]	Displays status and statistics of events which are subscribed to.
show grpc openconfig subscription	Displays information about static subscription association relationship (openconfig-telemetry.proto definition) of the device.

Command	Purpose
show grpc gnmi subscription	Displays information about subscription association relationship generated with the RPC method defined by gnmi.proto.
show grpc openr support-rpc	Displays openR RPC methods supported by the device.
show grpc yang tree	Displays the YANG model tree that is loaded by gRPC.
show grpc yang node-path	Displays paths corresponding to YANG nodes.

1.14 Configuration Examples

1.14.1 Configuring Basic Functions of gRPC

1. Requirements

A tested device is connected to a server and reports gRPC data.

2. Topology

Figure 1-4 Example of gRPC

3. Notes

- Ensure that the device and the PC are mutually reachable via the L3 route.
- Enable the gRPC function on the device.
- On the device, configure data in which the server must be reported.

4. Procedure

(1) Configure that the device and the PC are mutually reachable via the L3 route.

```
Device> enable
Device#configure terminal
Device(config)#interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 192.168.1.100 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
```

(2) Configure the gRPC function.

Enable the gRPC function.

```
Device(config)# grpc
```

Configure gRPC to bind a specified interface to send packets.

```
Device(config-grpc)# subscr-source-interface GigabitEthernet 0/1
```

(3) Configure data in which the server must be reported.

Configure the aaa new-model and the appropriate mlist test.

```
Device(config-grpc)# authen login authentication test
```

Configure realtime events of concern which are subscribed to.

```
Device(config-grpc)# subscr realtime enable
```

Configure the gRPC data response timeout time.

```
Device(config-grpc)# reply-timeout 30
```

Enable the heartbeat mechanism, configure a heartbeat period and an interval, and specify a channel and subscription type.

```
Device(config-grpc)# heartbeat inform interval 1 keepalive-times 1
Device(config-grpc)# user-server 192.168.1.1 12345
Device(config-grpc-us)# type 0x10000000 value 10
Device(config-grpc-us)# exit
```

Configure user login information of the specified server.

```
Device(config-grpc)# user-client 12345 test-user 192.168.1.100
```

Configure a YANG model path.

```
Device(config-grpc)# sensor-group 1
Device(config-grpc-us)# sensor-path
/rg-bridge:bridge/vlan/entry[id='1']/swport-list
Device(config-grpc-us)# exit
```

Configure a destination group.

```
Device(config-grpc)# destination-group 1
```

Configure an IPv4 address and port number of the destination group.

```
Device(config-grpc-destination)# ip 192.168.0.1 port 12345
```

Enable the destination group to use the gRPC protocol that supports TLS encryption.

```
Device(config-grpc-destination)# protocol grpc tls
Device(config-grpc-destination)# exit
```

Configure the subscription association relationship group, associated YANG model group and period interval, associated destination group, and data encoding format json-ietf.

```
Device(config-grpc)# subscription 1
Device(config-grpc-subscription)# sensor-group 1 sample-interval 1000
Device(config-grpc-subscription)# destination-group 1
Device(config-grpc-subscription)# encoding json-ietf
Device(config-grpc-subscription)# exit
```

Configure an RPC method defined by gnmi.proto.

```
Device(config-grpc)# rpc gnmi enable
```

Configure an RPC method defined by openR.

```
Device(config-grpc)# rpc openr enable
```

Configure a private RPC method to receive and send messages.

```
Device(config-grpc)# dial-out rpc gnmi-ext
```

5. Verification

Run the **ping** command to check whether the device and the PC are reachable via the L3 route.

```
Device# 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 = 2/3/5 ms.
```

Run the **show grpc status** command to check whether the gRPC function is enabled.

```
Device# show grpc status
GRPC:
  Uptime: 00h:28m:21s
```

Run the **show grpc client** command to display the user login information of the gRPC server.

```
Device# show grpc client
Client information all:
  1    : test-user@192.168.1.100, ID 12345
```

Run the **show grpc channel counter** command to display the statistics about the subscription server.

```
Device# show grpc channel counter
Server subscr all:
  server ip 192.168.1.1 port 50051
    state TRANSIENT_FAILURE
    heartbeat state FAILURE
  json list count: 0
  json send count: 1
  json drop count: 0
  call list count: 0
  call send count: 1
  call drop count: 0
```

Run the **show grpc channel counter** command to display the address, port number, and subscribing events of the subscription server.

```
Device# show grpc channel
Server subscr all:
  server ip 192.168.1.1 port 50051
    state TRANSIENT_FAILURE
    heartbeat state FAILURE
  subscr event:
    none
```

Run the **show grpc openconfig subscription** command to display the subscription relationship implemented according to openconfig-telemetry.yang.

```
Device# show grpc openconfig subscription
```

```
all subscriptions:
 subscription 1:
  sensor group 1:
    sample interval:1000
    sample timer count:858
    sensor path: /rg-bridge:bridge/vlan/entry[id='1']/swport-list
      state: NORMAL
      recv count: 858
  destination group 1:
    destination: 192.168.1.100:12345
      state: TRANSIENT_FAILURE
      task list count: 0
      task drop count: 0
      send request count: 0
      send update count: 0
      recv response count: 0
    destination: [1::1]:12345
      state: TRANSIENT_FAILURE
      task list count: 0
      task drop count: 0
      send request count: 0
      send update count: 0
      recv response count: 0
```

6. Configuration Files

- Device configuration file

```
hostname Device
!
grpc
 dial-out rpc gnmi-ext
 rpc gnmi enable
 rpc openr enable
 subscr realtime enable
 reply-timeout 30
 subscr-source-interface Mgmt 0
 user-client 12345 test-user 192.168.1.100
 heartbeat inform interval 1 keepalive-times 100
 sensor-group 1
  sensor-path /rg-bridge:bridge/vlan/entry[id='1']/swport-list
  exit-sensor-group
 destination-group 1
  protocol grpc tls
  ip 192.168.1.100 port 12345
  exit-destination-group
 subscription 1
  sensor-group 1 sample-interval 1000
```

```
  destination-group 1
  encoding json-ietf
  exit-grpc-subscription
 user-server 192.168.1.1 50051
  exit-user-server
!
end
```

Contents

1 Configuring OpenFlow 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Principles 1
1.1.3 Protocols and Standards 4
1.2 Restrictions and Guidelines 4
1.3 Configuration Task Summary 5
1.4 Configuring OpenFlow 5
1.4.1 Overview 5
1.4.2 Configuring OpenFlow 5
1.4.3 Configuring the OpenFlow Multi-controller Mode 5
1.4.4 Configuring the VLAN Tag for Packets Sent to the Controller 6
1.4.5 Configuring the Table-Lookup Mode 6
1.4.6 Configuring the OpenFlow Source IP Address 7
1.5 Monitoring 7
1.6 Configuration Examples 8
1.6.1 Configuring Central Control 8

1 Configuring OpenFlow

1.1 Introduction

1.1.1 Overview

OpenFlow is a network transmission protocol defined between a controller and the forwarding layer in the software defined network (SDN) architecture. OpenFlow allows the controller to directly access and operate network devices on the forwarding plane. These devices may be physical or virtualized.

OpenFlow separates the control plane from the forwarding plane of the network devices through standard communication protocols. Thus, the network devices focus on forwarding, and the control of an entire network focuses one controller. An OpenFlow connection is established between a controller and a device. The controller generates and delivers forwarding rules to the network device in a flow table through the OpenFlow connection, thereby centrally manage the control plane and reducing maintenance and management costs.

1.1.2 Principles

1. Basic Concepts

- Flow table

  A flow table is a core data structure for a device to control forwarding policies. Based on the flow table, the device determines an action to be taken for network traffic that enters the device.

  A device can have one or multiple flow tables. At present, a device supports only one flow table. A flow table is composed of multiple flow entries.

  According to the OpenFlow protocol, a flow entry consists of three parts: **header**, **counter**, and **action**.

  - **header**: It defines the index of a flow entry and consists of various packet fields such as source Media Access Control (MAC) address, destination MAC address, Ethernet protocol type, source IP address, destination IP address, IP protocol type, source port, and destination port. If a packet matches the header field of a flow entry, the packet matches this flow entry.
  - **counter**: It counts the number of packets and bytes that match this flow entry.
  - **action**: It defines an action taken for the packet that matches the flow entry, for example, discarding, broadcasting, or forwarding the packet.

- Message

  The OpenFlow protocol supports three categories of messages: **controller-to-switch**, **asynchronous**, and **symmetric**. Each category of messages include several subtypes of messages. The three categories of messages are described as follows:

  - **controller-to-switch**: This category of messages are initiated by the controller to manage and obtain network device statuses. For the subtypes of messages, see Table 1-1.
  - **asynchronous**: This category of messages are initiated by a network device to update network events or network device status changes (most commonly link up/down of a network port) to the controller. For the subtypes of messages, see Table 1-2.
  - **symmetric**: This category of messages are initiated either by a device or a controller to achieve an

initial handshake of the protocol and detect connection statuses. For the subtypes of messages, see Table 1-3.

Table 1-1 Subtypes of controller-to-switch Messages

Subtype	Description
Features	Used by a controller to send Features requests to understand device capabilities and responses.
Configuration	Used by a controller to query device configuration and make responses.
Modify-State	Used to manage device statuses, for example, flow entry and port statuses. This type of messages are used to add, delete, and modify flow entries, group entries, and port attributes of a device.
Multipart	Used by a controller to request device information, for example, current configuration and statistics.
Packet-Out	Used by a controller to send packets to a device.
Barrier	Used to check whether an action taken before a barrier message is successful. A controller sends a barrier request message. If a device confirms that the preceding action is successful, the device returns a barrier response message.
Role-Request	Used by a network device to request the role of a controller.
Asynchronous-Configuration	Used by a controller to set an asynchronous message filter and filter out unwanted asynchronous messages or query this filter.

Table 1-2 Subtypes of Asynchronous Messages

Subtype	Description
Packet-in	Used by a device to send packets to the controller.
Flow-Removed	Used to notify a controller of removing a flow entry from the flow table.
Port-Status	Used to notify a controller of the change in the device port status or configuration.
Error	Used to notify a controller of a device fault or error.

Table 1-3 Subtypes of Symmetric Messages

Subtype	Description
Hello	A message for interaction sent by between a controller and a device when an OpenFlow connection is established.

Subtype	Description
Echo	Keep-alive (echo request/reply) messages sent by a controller and a device.
Experimenter	A message reserved for new features.

2. Roles of the Controller

Table 1-4 Roles of the Controller

Role	Permission
Master	The controller in this role has all the permissions to control devices, deliver a flow table, query statistics, and receive status messages reported by the devices. In the cluster deployment mode, only one controller plays the master role.
Equal	The controller in this role has all the permissions of the controller. Compared with the master role, the equal role can be played by multiple controllers.
Standby	The controller in this role has partial permissions, and it is not permitted to deliver flow entries, group entries, or meter entries. The controller is not permitted to modify device configuration or perform packet out operation.

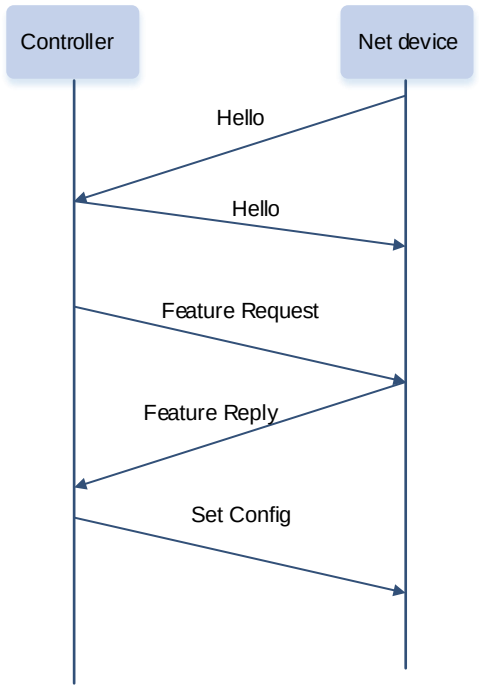
3. Separating Control from Forwarding

OpenFlow enables centralized management of the network control plane, so that the entire network can be centrally managed at ease (as compared with the status quo of the network), reducing maintenance and management costs.

The controller sends flow table information to the network devices, so as to control the method for forwarding network data packets and configuration parameters. Each network device will send a notification message to the controller when its link is interrupted or when the network device receives a data packet in which no forwarding action has been specified. In this way, the interaction between the controller and the network devices is implemented to eventually control the transmission of the entire network.

The mutual discovery between a controller and a network device must be completed before the controller and the network device interact with each other. Figure 1-1 shows the specific actions involved in this process.

Figure 1-1 Principle of the Controller and Network Device Interaction



Hello packets are sent between a controller and a network device to achieve a handshake. After the handshake is completed, the controller requests specific information about the device, including the number of ports on the network device and the capability of each port (such as the Feature Request/Reply shown in Figure 1-1). Then the controller delivers configurations (such as Set Config shown in Figure 1-1) to the specific network device. After a connection is established, the controller defines various flows and corresponding actions for the flows, and delivers them in a flow table to the network device. When a data packet enters the network device, the network device matches the data packet with the flow table according to present flow table rules and performs a corresponding action (including forwarding, discarding, and modifying the packet). At the same time, a corresponding counter is updated. If no match is found in the flow table, the network device forwards the data packet to the controller.

The network device locally maintains the flow table delivered from the controller. If the data packet to be forwarded is already defined in the flow table, the network device directly forwards the data packet. Otherwise, the data packet is sent to the controller to confirm the transmission path (which can be understood as control plane parsing to generate the flow table) and then forwarded based on the flow table delivered from the controller.

1.1.3 Protocols and Standards

- OpenFlow Switch Specification Version 1.0.0
- OpenFlow Switch Specification Version 1.3.0

1.2 Restrictions and Guidelines

- Only the Table 0 flow table is supported.
- A maximum of three controllers can be connected.

1.3 Configuration Task Summary

OpenFlow configuration includes the following tasks:

(1) Configuring OpenFlow

(2) (Optional) Configuring the OpenFlow Multi-controller Mode

(3) (Optional) Configuring the VLAN Tag for Packets Sent to the Controller

(4) (Optional) Configuring the Table-Lookup Mode

(5) (Optional) Configuring the OpenFlow Source IP Address

1.4 Configuring OpenFlow

1.4.1 Overview

As a network transmission protocol, OpenFlow runs over Transport Layer Security (TLS) or unprotected TCP connections, and defines the interaction between a controller and a network device.

1.4.2 Configuring OpenFlow

1. Overview

After the OpenFlow function is enabled on a device, packet forwarding control policies are generated and delivered by a controller.

2. Restrictions and Guidelines

- Before switching the address of a controller, disable and then enable the OpenFlow function again.
- When the OpenFlow function is enabled, the LLDP function on the device must be disabled. Otherwise, the LLDP packets delivered by a controller cannot be sent out.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the OpenFlow function.

of controller-ip *ipv4-address* [**port** *port-number*] [**aux**] **interface** *interface-type interface-number*

The OpenFlow function is disabled by default.

1.4.3 Configuring the OpenFlow Multi-controller Mode

1. Overview

After the multi-controller mode is configured, multiple controllers can be connected once.

2. Restrictions and Guidelines

Before the multi-controller mode is configured, the OpenFlow function must be disabled first. The multi-controller mode can take effect after the OpenFlow function is enabled again.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Connect an OpenFlow device to the controller.

of mode { **single** | **multiple** }

An OpenFlow device works in multi-controller mode by default.

(4) (Optional) Configure the interval at which an OpenFlow device reconnects to a controller.

of connect-interval *interval*

The default interval at which an OpenFlow device reconnects to a controller is 6 seconds.

(5) (Optional) Configure the echo request sending interval of an OpenFlow device.

of echo-interval *interval*

The default echo request sending interval of an OpenFlow device is 5 seconds.

1.4.4 Configuring the VLAN Tag for Packets Sent to the Controller

1. Overview

This function is used to configure a VLAN tag for packets sent to a controller by a device. Packets sent to a controller by a device contain the VLAN tag by default.

2. Restrictions and Guidelines

The configuration takes effect immediately.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a VLAN tag for packets sent by an OpenFlow device to a controller.

of packet vlantag

Packets sent to a controller by an OpenFlow device contain the VLAN tag by default.

1.4.5 Configuring the Table-Lookup Mode

1. Overview

This function is used to enable the table-lookup mode for received packets. A device looks up the flow table for the received packets by default, and processes the packets based on the matched entry. If no entry is matched, the packets are discarded.

2. Restrictions and Guidelines

The configuration takes effect immediately.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Connect an OpenFlow device to a controller.

of packet table-lookup { **enable** | **disable** }

The table-lookup mode is enabled for a network device by default.

1.4.6 Configuring the OpenFlow Source IP Address

1. Overview

The IP address of a device is configured as a source IP address for connecting to a controller. The default source IP address is the IP address of the connection port.

2. Restrictions and Guidelines

The configuration takes effect immediately and the network device is disconnected from the controller. Then, the source IP address is used for reconnection.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a source IP address for connecting an OpenFlow device to a controller.

of source-ip *ipv4-address*

The IP address of the connection port is the source IP address for connecting to a controller by default.

1.5 Monitoring

Run the **show** command to display the configuration.

Run the **clear** command to delete flow tables of devices.

Note

During device operation, running the **clear** command may cause service interruption due to key information loss.

Table 1-5 Monitoring

Command	Purpose
clear of-flow { all | sln-ac | sln-sc | xid *xid-number* **}**	Clears flow tables of the OpenFlow device.

Command	Purpose
clear of statistics	Clears OpenFlow statistics.
show of	Displays the status of the connection between an OpenFlow device and a controller.
show of port	Displays port information about the OpenFlow device.
show of flowtable	Displays the flow table of the current OpenFlow device.
show of group (only available in OpenFlow 1.3)	Displays the group table of the current OpenFlow device.
show of memory	Displays information about the memory dynamically applied by OpenFlow.
show of meter (only available in OpenFlow 1.3)	Displays the meter table of the current OpenFlow device.
show of mergedflow(only available in OpenFlow 1.3)	Displays the merged flow table of the current OpenFlow device.
show of rdnd	Displays OpenFlow real-time hot standby information.
show of runstatus	Displays key global data of an OpenFlow device during runtime.
show of sql	Displays information about the OpenFlow database.
show of statistics	Displays OpenFlow statistics.

1.6 Configuration Examples

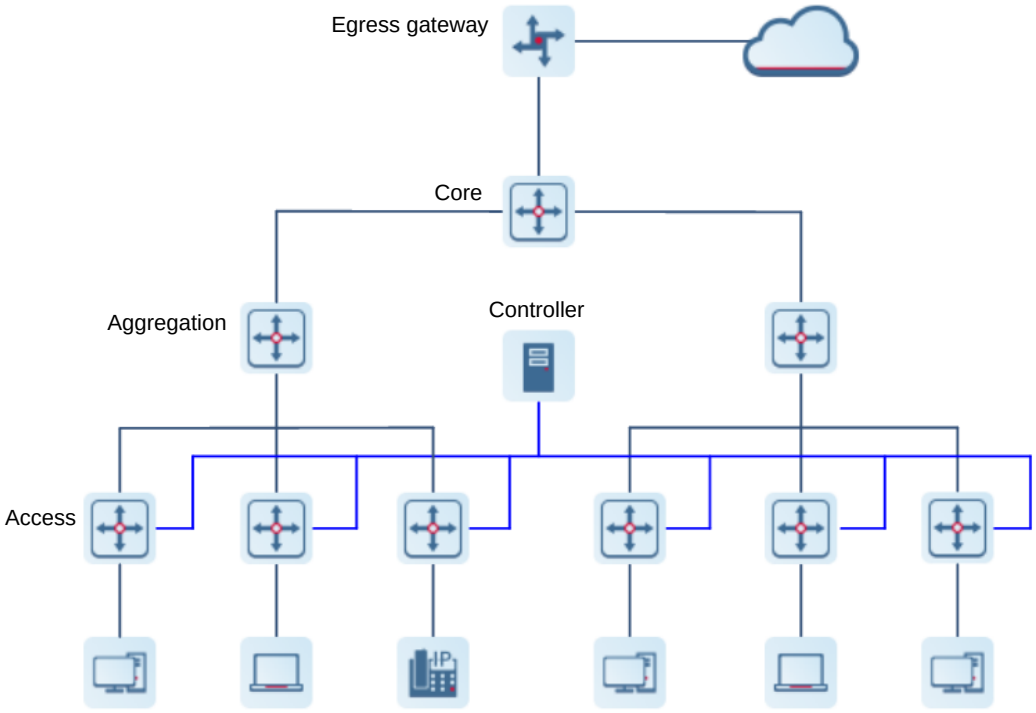
1.6.1 Configuring Central Control

1. Requirements

OpenFlow can be used to perform centralized management of access device authentication. As shown in Figure 1-2, a controller is deployed on an access device to authenticate and control the access device, so that the authentication function (on the control plane) is shifted from the access device to the controller.

2. Topology

Figure 1-2 Topology of Central Control



3. Notes

- Enable the OpenFlow function on a device and establish an OpenFlow management channel with a controller.
- Run OpenFlow Client on the access device to interconnect with the controller.
- The controller asks the access device to send an authentication packet to itself over the OpenFlow protocol.
- The controller completes the authentication process, and sends authentication results to the access device over the OpenFlow protocol to complete admission control on end users.

4. Procedure

Enable the OpenFlow function on a device, set the IP address of a controller to 172.18.2.36/24 and the port number to 65535, and disable the LLDP function on the device.

```
Device> enable
Device# configure terminal
Device(config)# no lldp enable
Device(config)# interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1))# no switchport
Device(config-if-GigabitEthernet 0/1))# ip address 172.18.2.36 255.255.255.0
Device(config-if-GigabitEthernet 0/1))# exit
Device(config)# of controller-ip 172.18.2.35 port 65535 interface GigabitEthernet 0/1
```

Configure the single-controller mode on the device.

```
Device(config)# of mode single
```

Remove the VLAN tag from packets sent to the controller.

```
Device(config)# no of packet vlantag
```

Configure the table-lookup mode on the device.

```
Device(config)# of packet table-lookup enable
```

Set the OpenFlow source IP address for the device to 192.168.197.25.

```
Device(config)# of source-ip 192.168.197.25
```

5. Verification

Display the connection status of OpenFlow 1.3.

```
Device# show of
version:openflow, controller[0]:tcp:172.18.2.35 port 65535 interface
FiveGigabitEthernet 0/1, main is connected, aux is disable,
Current controller mode : multiple.
Current packet process mode : Lookup all flow.
Datapath id = 123432320881645
Source IP = 192.168.197.25
Reconnect interval : 6 seconds.
Echo interval : 5 seconds
```

Display the port status of OpenFlow 1.3.

```
Device# show of port
ID    IFX    INTERFACE          SPEED    LINK    DUPLEX    TX_PKT      RX_PKT
CONFIG
1     1      GigabitEthernet 0/1  Unknown   DOWN    Unknown    0           0
NA
2     2      GigabitEthernet 0/2  Unknown   DOWN    Unknown    0           0
NA
3     3      GigabitEthernet 0/3  Unknown   DOWN    Unknown    0           0
NA
4     4      GigabitEthernet 0/4  Unknown   DOWN    Unknown    0           0
NA
5     5      GigabitEthernet 0/5  Unknown   DOWN    Unknown    0           0
NA
6     6      GigabitEthernet 0/6  Unknown   DOWN    Unknown    0           0
NA
7     7      GigabitEthernet 0/7  Unknown   DOWN    Unknown    0           0
NA
8     8      GigabitEthernet 0/8  Unknown   DOWN    Unknown    0           0
NA
9     9      GigabitEthernet 0/9  Unknown   DOWN    Unknown    0           0
NA
10    10     GigabitEthernet 0/10 Unknown   DOWN    Unknown    0           0
NA
```

```
11    11    GigabitEthernet 0/11 Unknown   DOWN    Unknown    0          0
NA
12    12    GigabitEthernet 0/12 Unknown   DOWN    Unknown    0          0
NA
13    13    GigabitEthernet 0/13 Unknown   DOWN    Unknown    0          0
NA
14    14    GigabitEthernet 0/14 Unknown   DOWN    Unknown    0          0
NA
15    15    GigabitEthernet 0/15 Unknown   DOWN    Unknown    0          0
NA
16    16    GigabitEthernet 0/16 Unknown   DOWN    Unknown    0          0
NA
```

Display the flow table status of OpenFlow 1.3.

```
Device# show of flowtable
/***************** openflow flow table[0]---flow number[2] ******************/

{table="0", duration_sec="5222", priority="0", flags ="0x1",idle_timeout="0",
hard_timeout="0", cookie="0x0", packet_count="0", byte_count="0". match=oxm{all
match} instructions=[apply{acts=[output{port="controller", max_len="3333"}] }] }
xid=472, sync_flag=0x0, ss_index=0x7b6

{table="0", duration_sec="5222", priority="66", flags ="0x1",idle_timeout="0",
hard_timeout="0", cookie="0x0", packet_count="0", byte_count="0".
match=oxm{eth_dst="00:25:64:c4:54:e4", eth_type="0x800", ipv4_dst="1.1.0.0",
ipv4_dst_mask="255.255.240.0"} instructions=[apply{acts=[output{port="controller",
max_len="65535"}] }] }
xid=473, sync_flag=0x0, ss_index=0x7b1

/***************************** openflow flow table end
*************************************/
flow total number = 2
```

Configure the single-controller mode on the device. The device can be connected to only one controller. If more controllers are connected, a notification will be displayed.

```
Device(config)# no of controller-ip
Device(config)# of mode single
Device(config)# of controller-ip 172.18.122.24 interface gigabitEthernet 0/1
Device(config)# of controller-ip 172.18.122.25 interface gigabitEthernet 0/1
Controller Mode is Single, can't connected
```

Run the **show of** command to check whether the current mode is the table-lookup mode and whether the source IP address is 192.168.197.25.

```
Device# show of
version:openflow1.3, controller[0]:tcp:172.18.105.11 port 6653 interface
GigabitEthernet 1/0/7, main is connected, aux is disable, role is master.
Current controller mode : multiple.
Current packet process mode : Lookup all flow.
```

```
Datapath id = 897516188948
Source IP = 192.168.197.25
```

6. Configuration Files

```
hostname Device
!
no lldp enable
!
of source-ip 192.168.197.25
of controller-ip 172.18.2.35 port 65535 interface GigabitEthernet 0/1
no of packet vlantag
!
interface gigabitEthernet 0/1
no switchport
ip address 172.18.2.36 255.255.255.0
```

7. Common Errors

- The controller IP address is incorrectly configured.
- The TCP port of the controller is incorrectly configured.
- The IP address of the local management channel is not configured.

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 10

1.5 Configuration Examples 10

1.5.1 Configuring Basic CWMP Functions 10

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.

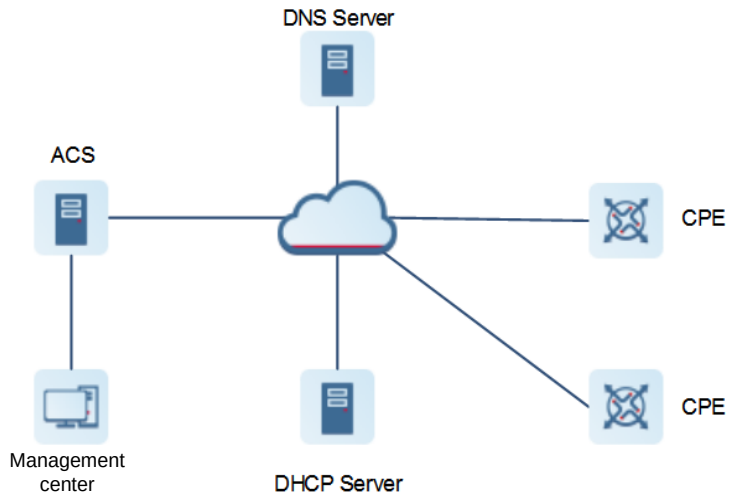
1.1.2 Principles

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

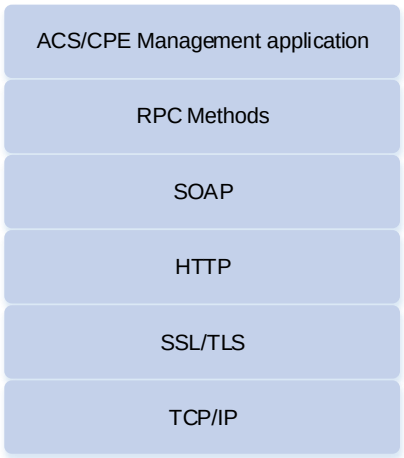
As shown in Figure 1-2, CWMP work is composed of six layers:

- 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.

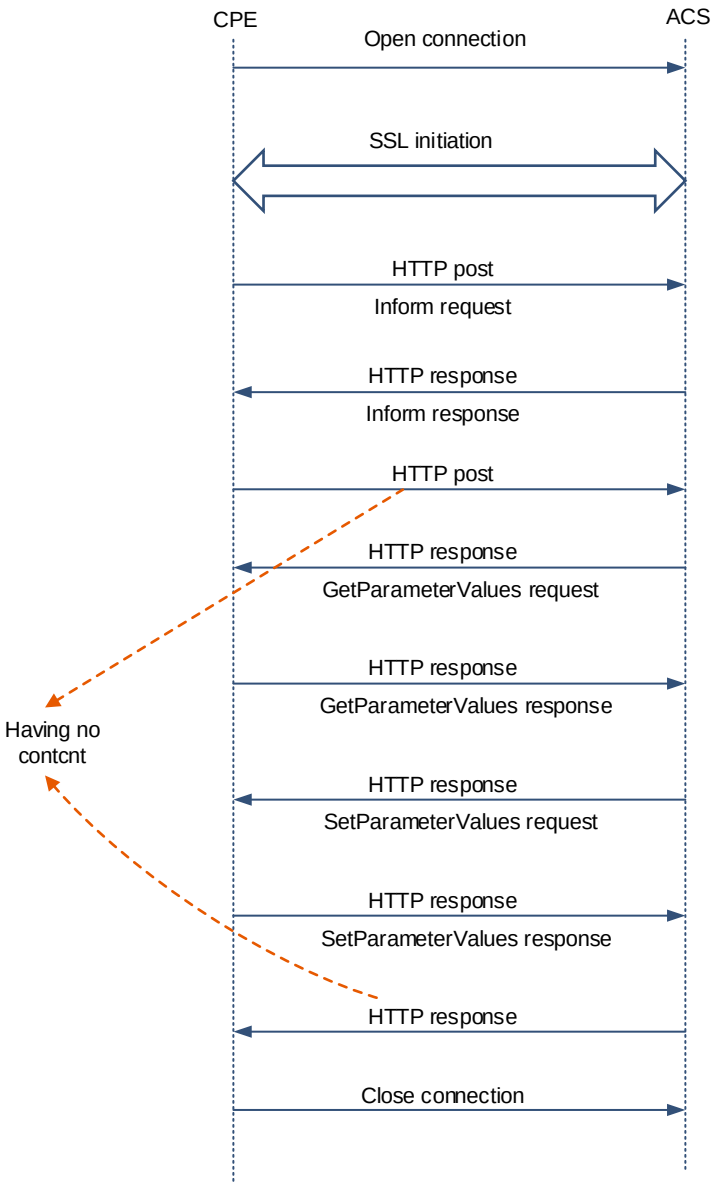
(7) When the ACS discovers that the ACS URL is not the local URL value, the ACS initiates a Set request, requesting the CPE to set its ACL URL to the URL value of the standby ACS.

(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 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.

- Pre-registration

  Pre-registration means that the CPE without configuration automatically connects to the ACS server and automatically goes online based on the CWMP configuration delivered by the ACS.

- 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. Before configuration, ensure that UDP port 7547 on the CPE is unused. This port is used for Simple Traversal of UDP over NATs (STUN) port listening. 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-password* | **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-password* | **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.
- The **no disable stun port-adaptive** command can be configured on the CPE to enable the STUN port auto-adaption function so that the CPE automatically adapts to ports 3478 and 3479 of the STUN server.

The **no disable stun probe-agingtime** command can be configured on the CPE to enable the NAT age time probe function. The CPE automatically binds with UDP port 7548, detects NAT age time and adjusts STUN port keep-alive time through this UDP port.

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 STUN port auto-adaption and NAT age time probe function.

  no disable stun { **port-adaptive** | **probe-agingtime** }

  The STUN port auto-adaption and NAT age time probe function is disabled by default.

- Configure the maximum keep-alive time of STUN packets.

  stun max-period *interval*

  The maximum keep-alive time of STUN packets is **60** seconds by default.

- Configure the minimum keep-alive time of STUN packets.

  stun min-period *interval*

  The minimum keep-alive time of STUN packets is **20** seconds by default.

- Configure a port of the STUN server.

  stun port *port-number*

  The default port ID of the STUN server is **3478**.

- Configure a STUN server address.
  stun address { *stun-domain-address* | *stun-ipv4-address* }

No STUN server address is configured 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.

- Enable the pre-registration function.

  register device

  The pre-registration function is disabled by default.

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

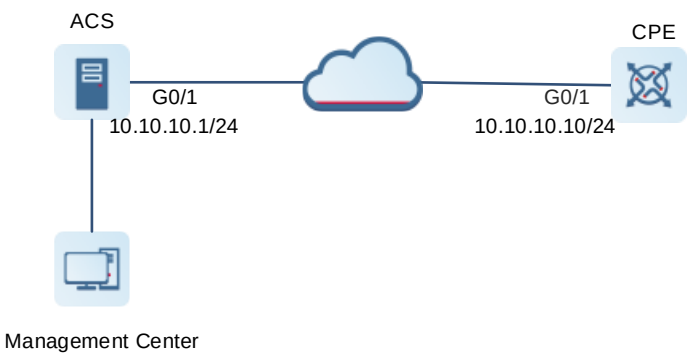
1.5.1 Configuring Basic CWMP Functions

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 gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.10.10.10 255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# exit
```

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 100 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
```

Enable the CWMP function and enter the CWMP configuration mode.

```
Hostname(config-cwmp)# no disable stun port-adaptive
```

Enable the STUN port auto-adaption and NAT age time probe function.

```
Hostname(config-cwmp)# no disable stun probe-agingtime
```

Configure the username and password of the ACS.

```
Hostname(config-cwmp)# acs username USERB
Hostname(config-cwmp)# acs password Abc123456
```

Configure the username and password of the CPE.

```
Hostname(config-cwmp)# cpe username USERB
Hostname(config-cwmp)# cpe password Abc123456
```

5. Verification

Run the **ping** command to check whether the CPE and ACS are mutually reachable via L3 routes.

```
Hostname# ping 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                 : $10$07b$/Qy2cVjc5r8n$
CPE source interface name      :
CPE URL                     : http://10.10.10.1:7547/
CPE username                 : USERB
CPE password                 : $10$07b$/Qy2cVjc5r8n$
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 address             :
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 7 $10$07b$/Qy2cVjc5r8n$
 cpe source interface GigabitEthernet 0/1
 cpe username USERB
 cpe password 7 $10$07b$/Qy2cVjc5r8n$
 timer cpe-timeout 100
```

```
 disable upload
 cpe back-up delay-time 30
 no disable stun port-adaptive
 no disable stun probe-agingtime
!
interface GigabitEthernet 0/1
 ip address 10.10.10.10 255.255.255.0
```

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 SPAN 1
1.1 Introduction 1
1.1.1 Overview 1
1.1.2 Basic Concepts 1
1.1.3 Principles 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 6
1.4.3 Procedure 6
1.5 Configuring RSPAN 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 9
1.7.1 Configuring SPAN 9
1.7.2 Configuring RSPAN to Realize One-to-Many SPAN 11

1 Configuring SPAN

1.1 Introduction

1.1.1 Overview

With the development of network technologies, the demand for high network availability is increasing. When exceptions occur in a network, the network node or device port needs to be analyzed for data traffic so that the network can return to normal fast. Meanwhile, the device traffic forwarding should not be affected.

The mirroring function copies messages from a specified port to another port connected to a network monitoring device. The device analyzes data traffic of a suspicious network node or device port, without affecting the traffic forwarding of the monitored device. Mirroring is mainly applied to network monitoring and troubleshooting to monitor network information for security and troubleshoot network failures.

1.1.2 Basic Concepts

1. Source Port

A source port is also called a monitored port. The data traffic of a source port is copied to a destination port for network analysis or troubleshooting.

2. Destination Port

A destination port is also called a monitoring port. A destination port is connected to a device to forward packets received from a source port to a monitoring device.

3. Session

A session is a logical concept, which consists of a source port and a destination port.

4. SPAN

Switch port analyzer (SPAN) is also called local port mirroring or local mirroring. In local port mirroring, the source port and the destination port in a mirroring session are in the same device.

5. RSPAN

Remote switch port analyzer (RSPAN) is an extension of SPAN. In RSPAN, the source port and the destination port in a mirroring session are in different devices.

6. RSPAN VLAN

An RSPAN VLAN is a special VLAN that only transmits mirrored packets to a destination device.

7. Output Port

An output port on a source device sends mirrored packets to a port on an intermediate device or a destination device.

8. Source Device

A source device is a role in RSPAN and has a source port. A source device copies the packets from a source port and outputs them through an output port on the source device to an intermediate device or destination device.

9. Destination Device

A destination device is a role in RSPAN and has a destination port. A destination device forwards the mirrored packets received from an intermediate or source device to a monitoring device through a destination port.

10. Intermediate Device

An intermediate device is a role in RSPAN and resides between a source device and a destination device. An intermediate device forwards mirrored packets to another intermediate device or a destination device. If a source device is directly connected to a destination device, there is no intermediate device.

11. SPAN Data Streams

SPAN data streams refer to mirrored packets. A SPAN session contains data streams in three directions:

- Input data streams

  All packets received by a source port are copied to a 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 a 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.

1.1.3 Principles

1. SPAN Principles

As shown in Figure 1-1, all packets on port 1 are copied to port 10 through configuring SPAN on Device A. The network analyzer connected to port 10 receives all packets that pass through port 1 even if the network analyzer is not directly connected to port 1. Therefore the network analyzer can monitor the data streams 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 1.

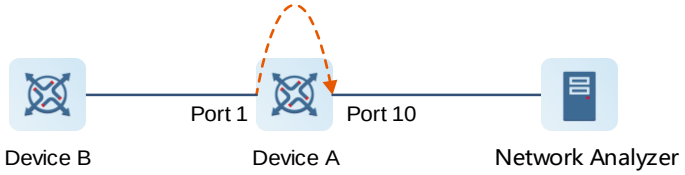
(2) The device searches for the SPAN session to which port 1 belongs.

(3) The device searches for the destination port 10 corresponding to the SPAN session.

(4) The device copies both incoming and outgoing packets of port 1 and sends them to port 10.

(5) Port 10 sends the copied packets to the network analyzer.

Figure 1-1 SPAN Principles



2. RSPAN Working Process

As shown in Figure 1-2, an RSPAN VLAN is created for the source device, intermediate device, and destination device. All ports involved in an RSPAN session must be added to the RSPAN VLAN. Mirrored packets are broadcast in the RSPAN VLAN so that they are forwarded from the source device to the destination device. Then the destination device forwards the mirrored packets to the network analyzer. The following is the specific working process.

(1) Add all ports involved in an RSPAN session of a source device, intermediate device, and destination device to an RSPAN VLAN.

(2) The source device adds the VLAN ID of the RSPAN VLAN to the mirrored packets of the source port. Then the device copies the encapsulated packets to the output port.

Note

As shown in Figure 1-3, for 1:N port mirroring, enable the loopback function on the output port of the source device to make it a loopback port. Add the loopback port (port 1) and the interface of the intermediate device (port 2) to the RSPAN VLAN. The source port adds the VLAN ID of the RSPAN VLAN to the mirrored packets and copies the packets to the loopback port. The loopback port belongs to the RSPAN VLAN and this VLAN is forbidden to learn any MAC address. Therefore the reflected packets are broadcast in the RSPAN VLAN so that all ports in this VLAN can receive the mirrored packets to achieve 1:N port mirroring .

(3) The output port sends the mirrored packets to a port on an intermediate device or a destination device.

(4) The intermediate device broadcasts mirrored packets in the RSPAN VLAN to transparently transmit the packets to another intermediate device or a destination device.

Note

If a source device is directly connected to a destination device, there is no intermediate device.

(5) After receiving the packets, the destination device determines whether they are mirrored packets through the VLAN ID. If the VLAN ID carried by the packets is the same as the RSPAN VLAN ID, the device regards the packet as a mirrored packet and forwards the packet to the network analyzer through the destination port.

Figure 1-2 Principles of RSPAN

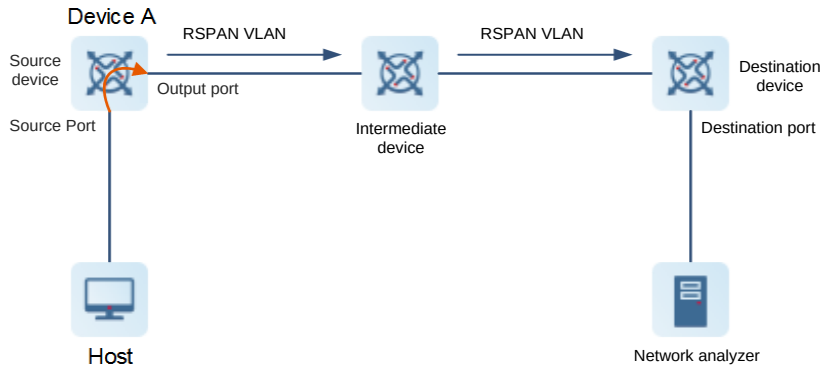
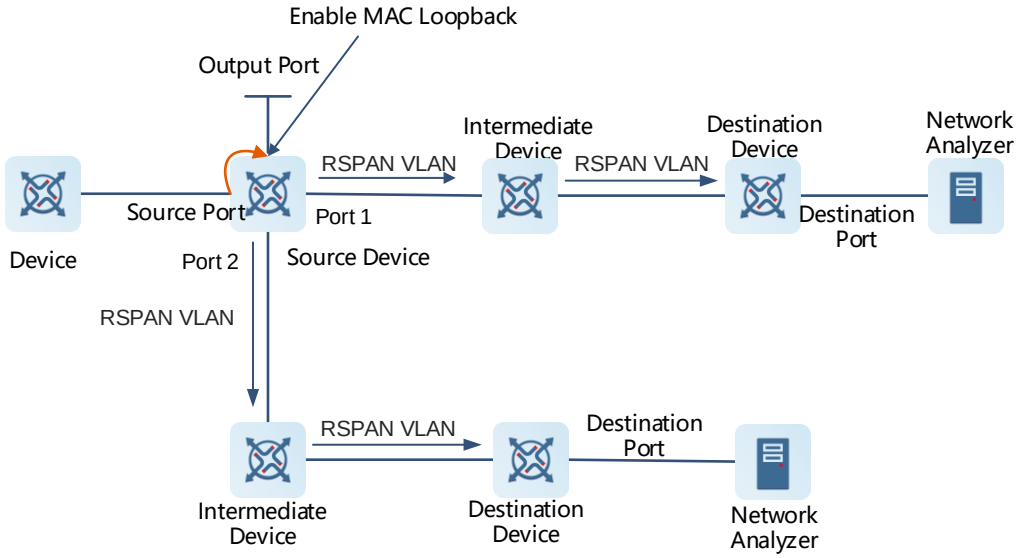


Figure 1-3 Principles of 1:N Port Mirroring Based on RSPAN



3. 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.

1.2 Restrictions and Guidelines

- A source port has the following features:
  - The source port and the output port cannot be the same one.
  - The source port can be a Layer 2 Ethernet interface, Layer 3 Ethernet interface, Layer 2 link aggregation or Layer 3 link aggregation.
  - Data streams on multiple source ports on the source device can be mirrored to a specified output port.
  - When the source port is a Layer 3 link aggregation or Ethernet interface, the port monitors both Layer 2 and Layer 3 packets.
  - 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.

  If a source port is added to a link aggregation, the source port exits the SPAN session. The source port acts as only a member port of the link aggregation.

- A destination port has the following features:
  - A destination port cannot be used as a source port simultaneously.
  - The destination port can be an Ethernet interface, link aggregation.
  - The SPAN destination port is used for the Spanning Tree Protocol (STP) calculation.
- A source port cannot be added to an output group.
- A configured session ID cannot be used as the ID of another 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.
- Configure ACLs on the source port to mirror specified packets.
- The device does not support secondary mirroring for the destination port. For example, if the source port of mirroring session 2 is configured as the destination port of mirroring session 1, session 2 cannot mirror mirroring packets of the source port.

1.3 Configuration Task Summary

SPAN configuration includes the following tasks:

- Configuring SPAN
- Configuring RSPAN

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 or 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.
- If the source and destination ports of mirroring are both configured as LACP aggregate ports, the LACP protocol oscillates repeatedly on the destination port and its peer port.

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* }

- (Optional) Exclude one or more VLANs as the data source of SPAN.

  monitor session *session-number* **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-number* **source vlan** *vlan-id-list* **rx**

  This function 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-number* **destination interface** *interface-type interface-number* [**switch**]

By default, no SPAN destination port is configured.

1.5 Configuring RSPAN

1.5.1 Overview

A device enabled with RSPAN can monitor packets acrorss networks for network monitoring and troubleshooting.

1.5.2 Restrictions and Guidelines

- All ports involved in RSPAN must be added to a remote VLAN.
- An RSPAN VLAN must be configured on each device and their VLAN IDs must be consistent. All ports involved in a session must be added to the VLAN. Do not add common ports to an RSPAN 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.
- To achieve 1:N port mirroring, configure a port on a source device as a loopback port. The loopback function on the output port will transmit mirrored packets to multiple intermediate devices or destination devices.
- The loopback port cannot serve as a normal port to forward packets. You are advised to configure a port in Down state as the loopback port, and not to add other configurations for this port.
- If the source and destination ports of mirroring are both configured as LACP aggregate ports, the LACP protocol oscillates repeatedly on the destination port and its peer port.
- When RSPAN is configured to mirror Layer 2 broadcast packets and the destination interface is an aggregate interface, if the aggregate interface has member interfaces across chips (including member interfaces across devices in VSU mode) and the load balancing mode is **src-dst-ip**, some traffic may fail to be forwarded through members of the aggregate interface, resulting in packet loss. If you need to mirror Layer 2 broadcast packets to an aggregate interface, use either of the following methods to avoid packet loss:
  - Change the load balancing mode of the aggregate interface to MAC-based load balancing.
  - Configure member interfaces of an aggregate interface on the same chip or the same device.

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-number* **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 Layer 2 Ethernet interface configuration mode or Layer 3 Ethernet 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) Exit the Layer 2 Ethernet interface configuration mode or Layer 3 Ethernet interface configuration mode.

exit

(9) Configure a source port on the source device.

monitor session *session-number* **source interface** *interface-type interface-number* [{ **both** | **rx** | **tx** } [**acl** { *acl-name* | *acl-number* }]

By default, no source port on the source device is configured for an RSPAN session.

(10) Configure an RSPAN destination device.

monitor session *session-number* **remote-destination**

By default, no destination device is configured for an RSPAN session.

(11) 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 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 monitor [**session** *session-number*]	Displays the SPAN session information.
show span-info information { **acl-ref** | **client** | **data-sync** | **global-info** | **memory** }	Displays debugging information of the SPAN module.

1.7 Configuration Examples

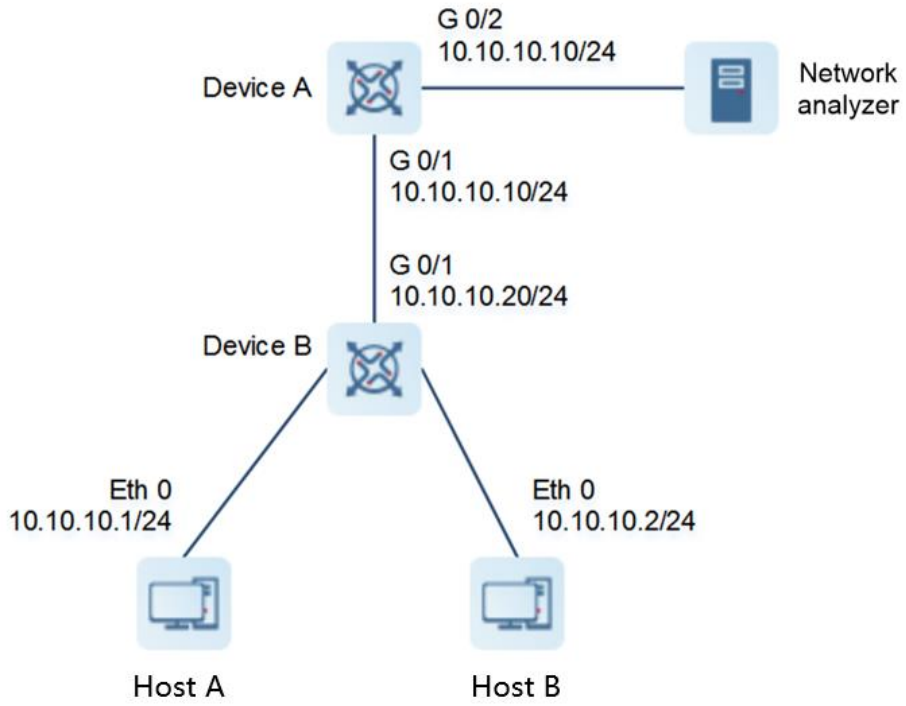
1.7.1 Configuring SPAN

1. Requirements

As shown in Figure 1-4, 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 Host A and Host B).

2. Topology

Figure 1-4 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 Host A and Host B 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

GigabitEthernet 0/1 and GigabitEthernet 0/2 of Device A belong to VLAN 1 by default.

On device A, create SVI 1 and set the address of SVI 1 to 10.10.10.10/24.

```
DeviceA> enable
DeviceA# configure terminal
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. The configuration details are not mentioned here.

On device B, create SVI 1 and set the address of SVI 1 to 10.10.10.20/24.

```
DeviceB# configure terminal
DeviceB(config)# vlan 1
Device B (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
```

1.7.2 Configuring RSPAN to Realize One-to-Many SPAN

Caution

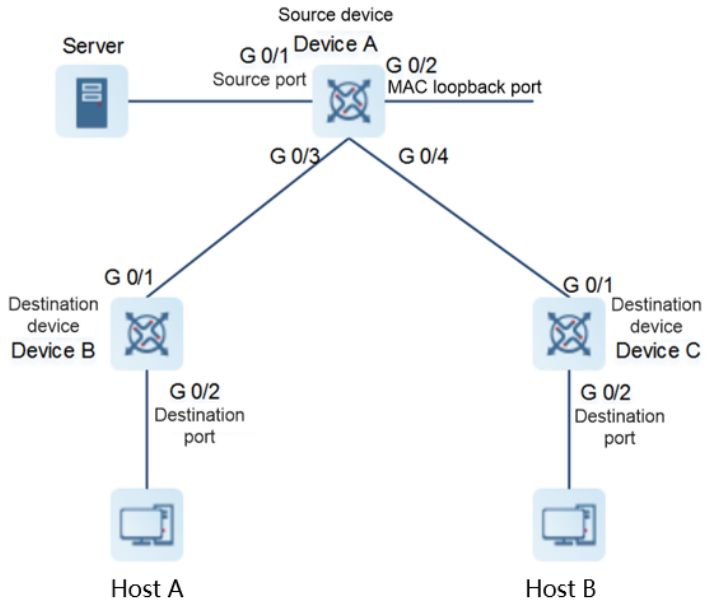
When deploying One-to-Many SPAN, you must run the **switchport trunk allowed vlan remove** *vlan-list* command to remove the broadcast VLANs from a trunk interface on each SPAN device. Otherwise, the trunk interface may be fully occupied by the broadcast traffic, causing service interruption.

1. Requirements

As shown in Figure 1-5, the RSPAN function enables the network analyzer to monitor bidirectional data streams of the source device A from the destination devices B and C. The devices can normally exchange data with each other.

2. Topology

Figure 1-5 Topology of RSPAN Used to Realize One-to-Many SPAN



3. Notes

- Configure device A as the source device. Configure an RSPAN VLAN. Configure GigabitEthernet 0/1 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 1:N SPAN. Configure the switching function of the output port.
- Configure devices B and C as the destination devices. Configure an RSPAN 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 terminal
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.

```
Device B> 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 DeviceC
!
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.

Contents

1 Configuring RNS 1

1.1 Introduction 1

1.1.1 Principles 1

1.1.2 Protocols and Standards 3

1.2 Restrictions and Guidelines 3

1.3 Configuration Task Summary 3

1.4 Configuring Basic Features of RNS 3

1.4.1 Overview 3

1.4.2 Restrictions and Guidelines 3

1.4.3 Procedure 3

1.5 Configuring the ICMP Echo Test 5

1.5.1 Overview 5

1.5.2 Restrictions and Guidelines 5

1.5.3 Procedure 5

1.6 Configuring the UDP Echo Test 6

1.6.1 Overview 6

1.6.2 Restrictions and Guidelines 6

1.6.3 Procedure 6

1.7 Configuring the TCP Connection Test 6

1.7.1 Overview 6

1.7.2 Restrictions and Guidelines 6

1.7.3 Procedure 6

1.8 Configuring the DHCP Test 7

1.8.1 Overview 7
1.8.2 Restrictions and Guidelines 7
1.8.3 Procedure 7
1.9 Configuring the DNS Test 7
1.9.1 Overview 7
1.9.2 Restrictions and Guidelines 7
1.9.3 Procedure 7
1.10 Monitoring 8
1.11 Configuration Examples 9
1.11.1 Configuring Basic Functions of the ICMP Echo Test 9
1.11.2 Configuring Basic Functions of the UDP Echo Test 10
1.11.3 Configuring Basic Functions of the TCP Connect Test 12
1.11.4 Configuring Basic Functions of the DHCP Test 14
1.11.5 Configuring Basic Functions of the DNS Test 16
1.12 Common Misconfigurations 17
1.12.1 No Packet Is Obtained After RNS Configuration Is Completed 17

1 Configuring RNS

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.

1.1.1 Principles

1. RNS Test

An RNS test can be regarded as an RNS process. Before performing an RNS test, you must create an RNS test. In the RNS test, you need to configure RNS parameters, such as the test type, test destination address, and test frequency. The instance ID is globally unique. You need to configure test parameters based on the test type. The detection types include ICMP echo test, UDP echo test, TCP connect test, DHCP test, and DNS test.

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.

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.

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.

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.

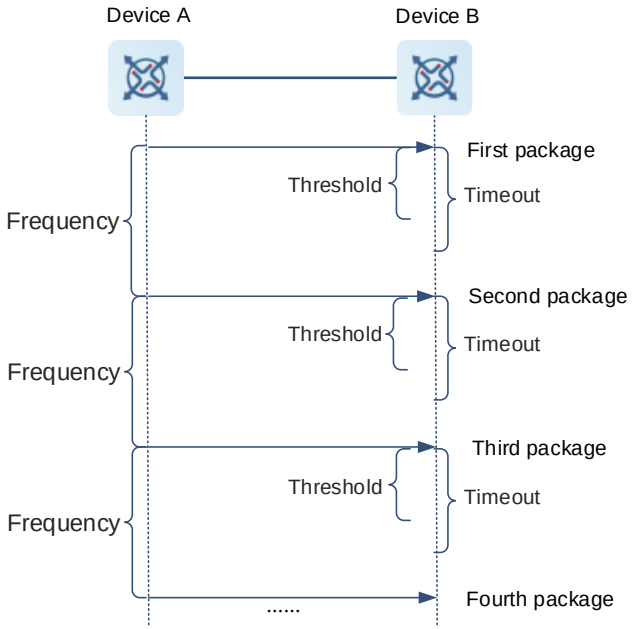
6. DNS Test

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.

7. Test Packet Sending Mechanism

- Continuous test
  - Definition: Packets are sent at a specified frequency within the specified lifetime, and the timeout interval of each packet is specified, which are used for collecting the delay, jitter, and packet loss rate.
  - Applicable test types: ICMP Echo, UDP Echo, TCP Connect, DHCP, and DNS
  - Details: If no response packet is received within the timeout interval after a request packet is sent, the request packet is lost and marked as lost. Figure 1-1 illustrates the packet sending mechanism.
  - Constraint: Threshold ≤ Timeout < Frequency

Figure 1-1 Continuous Test Packet Sending Mechanism



1.1.2 Protocols and Standards

RFC 2925: Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations.

1.2 Restrictions and Guidelines

- In IP RNS configuration mode, if you do not configure the test type, the RNS test instance is not created.
- After configuring an RNS test instance, you need to run the **ip rns schedule** command to configure a policy for enabling the instance. Otherwise, the test will not be executed.
- ICMP Echo test, TCP Connect test, and UDP Echo test support IPv4 and IPv6, but DNS test and DHCP test support only IPv4.

1.3 Configuration Task Summary

RNS configuration includes the following tasks:

(1) Configuring Basic Features of RNS

(2) Configuring the ICMP Echo Test

(3) Configuring the UDP Echo Test

(4) Configuring the TCP Connection Test

(5) Configuring the DHCP Test

(6) Configuring the DNS Test

1.4 Configuring Basic Features of RNS

1.4.1 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.

1.4.2 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.

1.4.3 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 for the RNS test. Select at least one of the following configuration tasks.

- Configure the threshold monitoring and triggering mechanism when monitoring all elements fails.

  ip rns reaction-configuration *operation-number* **react allfail** [**action-type track** | **threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*] }] *

- Configure the threshold monitoring and triggering mechanism when the packet round trip time is not within the threshold range.

  ip rns reaction-configuration *operation-number* **react rtt** [**action-type** { **trigger** | **none** } | **threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*] } | **threshold-value** *upper-threshold lower-threshold*] *

- Configure the threshold monitoring and triggering mechanism based on the timeout in either direction.

  ip rns reaction-configuration *operation-number* **react timeout** [**action-type** { **trigger** | **none** } | **threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*] }] *

The proactive threshold monitoring and triggering mechanism is not configured for the test by default.

(5) Trigger another test in pending state to activate when the monitoring threshold exceeds the expectation during a test.

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.

1.5 Configuring the ICMP Echo Test

1.5.1 Overview

Create an RNS test instance of ICMP echo 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) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Create an RNS test instance of ICMP echo type.

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 virtual routing and forwarding (VRF) of an RNS test.

vrf *vrf-name*

No VRF name is configured for the test by default.

(10) 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.

1.6 Configuring the UDP Echo Test

1.6.1 Overview

Create an RNS test instance of UDP echo type and implement the UDP echo test.

1.6.2 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.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an RNS test instance of UDP echo type.

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 **vrf**) of configuring common optional parameters of a test, see 1.5 Configuring the ICMP Echo Test. They are omitted here.

1.7 Configuring the TCP Connection Test

1.7.1 Overview

Create an RNS test instance of TCP type to implement a TCP connection test.

1.7.2 Restrictions and Guidelines

- You must first configure the RNS basic features.
- The target host must be able to respond to the TCP connection request.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an RNS test instance of 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 **vrf**) of configuring common optional parameters of a test, see 1.5 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 1.5 Configuring the ICMP Echo Test. They are omitted here.

1.9 Configuring the DNS Test

1.9.1 Overview

Create an RNS test instance of DNS type.

1.9.2 Restrictions and Guidelines

You must first configure the RNS basic features.

1.9.3 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 *domain-hostname* **name-server** *ipv4-address* [[**af-direct**] **out-interface** *interface-type interface-number* [**next-hop** *ipv4-address*] | **source-ipaddr** *ipv4-address*] *

No test of DNS type is created by default.

Caution

For the commands (**frequency, tag, threshold, timeout** and **vrf**) of configuring common optional parameters of a test, see 1.5 Configuring the ICMP Echo Test. They are omitted here.

1.10 Monitoring

Run the **show** command to check the configuration.

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

Caution

Debugging occupies system resources, so disable it immediately if not required.

Table 1-1 RNS Monitoring

Command	Purpose
show ip rns configuration [**json**] [*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 [**json**] [*operation-number*]	Displays the brief statistics of one or more RNS instances.
debug rns { **all | interface | lib | rdnd-event | restart | rns_id** [**0, 500**] }	Debugs the RNS module.

Command	Purpose
debug rns-server {udp-echo} { event | fail | packet }	Debugs the RNS server module.

1.11 Configuration Examples

1.11.1 Configuring Basic Functions of 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 1-2 Topology for Configuring the ICMP Echo Test

3. Notes

Configure RNS test 1 and related parameters on Device A.

4. Procedure

(1) Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on each device to ensure that routes between the devices are reachable.

(2) Configure RNS test 1 and parameters.

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
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip rns 1
 icmp-echo 10.2.2.2
!
ip rns schedule 1 start-time now life forever
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.0.0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.2.2.2 255.255.0.0
!
end
```

1.11.2 Configuring Basic Functions of 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 1-3 Topology for Configuring the UDP Echo Test

3. Notes

Configure RNS test 1 and related parameters on Device A.

4. Procedure

(1) Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on each device to ensure that routes between the devices are reachable.

(2) Configure RNS test 1 and parameters.

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
```

(3) Configure the server of the UDP echo test.

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 test 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. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip rns 1
 udp-echo 10.2.2.2 1025
!
```

```
ip rns schedule 1 start-time now life forever
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.0.0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ip rns-server udp-echo 1025
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.2.2.2 255.255.0.0
!
end
```

7. Common Errors

The UDP server port configured on the client is not correct.

1.11.3 Configuring Basic Functions of 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 1-4 Topology for Configuring the TCP Connect Test

3. Notes

Configure RNS test 1 and related parameters on Device A.

4. Procedure

(1) Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on each device to ensure that routes between the devices are reachable.

(2) Configure RNS test 1 and parameters.

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 test 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. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip rns 1
 tcp-connect 10.2.2.2 8000
!
ip rns schedule 1 start-time now life forever
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.0.0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.2.2.2 255.255.0.0
!
end
```

7. Common Errors

- The target host does not respond to the TCP connection request.
- The configured TCP port for the RNS test is incorrect.

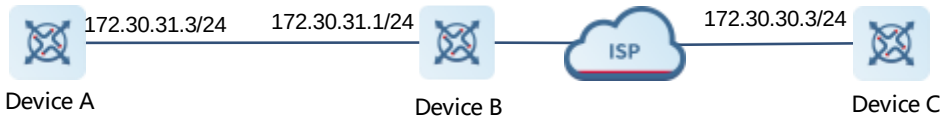
1.11.4 Configuring Basic Functions of the DHCP Test

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

(1) Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on each device to ensure that routes between the devices are reachable.

(2) Enable the DHCP server and configure address pool parameters.

Perform the following configuration on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# service dhcp
DeviceB(config)# ip dhcp pool test
DeviceB(dhcp-config)# network 10.2.0.0 255.255.0.0
DeviceB(dhcp-config)# end
```

(3) Configure RNS test 1 and parameters.

Perform the following configuration on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip rns 1
DeviceA(config-ip-rns)# dhcp 172.30.30.3 out-interface gigabitethernet 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 test 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 0/1
Next-hop address: 172.30.31.1
```

1. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip rns 1
 dhcp 172.30.30.3 out-interface GigabitEthernet 0/1 next-hop 172.30.31.1
!
ip rns schedule 1 start-time now life forever
!
interface GigabitEthernet 0/1
 no switchport
 ip address 172.30.31.3 255.255.0.0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
service dhcp
!
ip dhcp pool test
 network 10.2.0.0 255.255.0.0
!
interface GigabitEthernet 0/1
 no switchport
 ip address 172.30.30.1 255.255.0.0
!
End
```

- Device C configuration file

```
hostname DeviceC
!
interface GigabitEthernet 0/1
 no switchport
 ip address 172.30.30.3 255.255.0.0
!
end
```

6. Common Errors

- The DHCP service is not enabled on the server.
- No IP address is configured for the outbound interface of the client.

1.11.5 Configuring Basic Functions of the DNS Test

1. Requirements

Configure an RNS test of DNS type, which must be started immediately and take effect permanently.

2. Topology

Figure 1-6 Topology for Configuring the DNS Test

3. Notes

Configure RNS instance 1 and related parameters on Device A.

4. Procedure

(1) Configure interface IP addresses and an IPv4 unicast routing protocol (for example, OSPF) on each device to ensure that routes between the devices are reachable.

(2) Configure RNS test 1 and parameters.

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
```

(3) Enable the DNS proxy function.

Perform the following configuration on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# ip dns proxy enable
DeviceB(config)# exit
```

5. Verification

Run the **show ip rns configuration** command to display the test 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. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip rns 1
 dns www.abc.com name-server 10.2.2.2
!
ip rns schedule 1 start-time now life forever
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.0.0
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ip dns proxy enable
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.2.2.2 255.255.0.0
!
end
```

7. Common Errors

The DNS IP address is incorrect.

1.12 Common Misconfigurations

1.12.1 No Packet Is Obtained After RNS Configuration Is Completed

- Symptom

  After the RNS configuration is configured, no packet is obtained. The **show ip rns collection** command cannot be used to obtain detailed test information, or the number of sent or received packets is 0.

- Solution
  - Check whether the ping operation succeeds.

Run the **ping** command to check connectivity of the destination path.

- Check whether scheduling is configured and whether packets are sent at the specified scheduling time.

  Run the **ip rns schedule** *operation-number* **start-time now** command to enable scheduling. If no scheduling is performed, the configuration can be performed. Otherwise, a message indicating that the RNS test is running is displayed.

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....3
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....7
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.

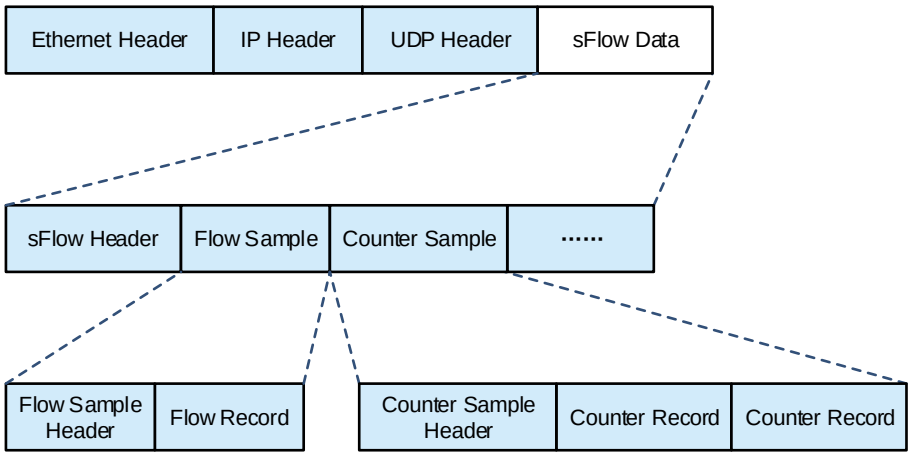
- **sFlow Collector**

  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

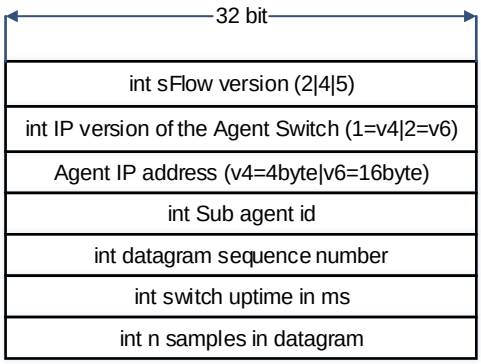


Table 1-1 sFlow Header Description

Field	Description
sFlow version	sFlow version. V2, V4, and V5 are available. Currently, the product 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.

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 an Ethernet interface or a link aggregation.
- **sFlow enable**
  - This command can be configured on an Ethernet interface or a link aggregation.
  - 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.
  - The ACL is supported only in the inbound direction. Configure the ACL before configuring this command.

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) Enter the interface configuration mode.

- Enter the Layer 2 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 2 link aggregation configuration mode.

  interface aggregateport *interface-number*

- Enter the Layer 3 Ethernet interface configuration mode.

  interface *ethernet-type interface-number*

- Enter the Layer 3 link aggregation configuration mode.

  interface aggregateport *interface-number*

(6) Configure the ID of the sFlow Collector for flow sampling. Configure at least one of the following task.

- 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.

- 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 sampling functions.

sflow enable [{ **ingress** [**acl** *acl-name* | **acl** *acl-number*] | **egress** }]

The sFlow sampling 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 of a packet, 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) (Optional) 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) (Optional) Configure the sFlow flow sampling rate.

sflow sampling-rate *sampling-rate*

The default sFlow flow sampling rate is **8192**.

(5) (Optional) 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) (Optional) 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) (Optional) 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	Displays the sFlow capacity supported by the device.

1.5 Configuration Examples

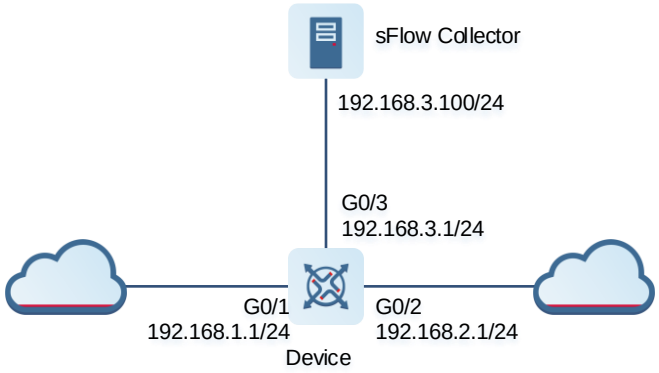
1.5.1 Configuring Basic Functions of sFlow

1. Requirements

Start the device that serves as the sFlow Agent, enable flow sampling and counter sampling on port GigabitEthernet 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 Network of Basic sFlow Configuration



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:65536
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

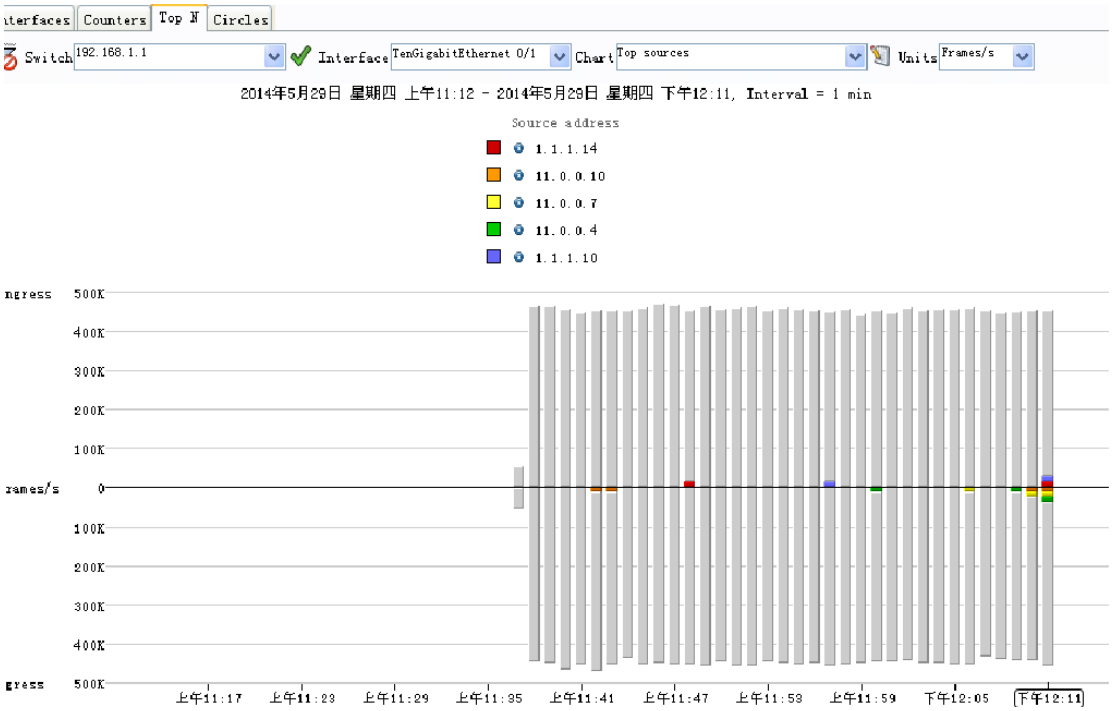
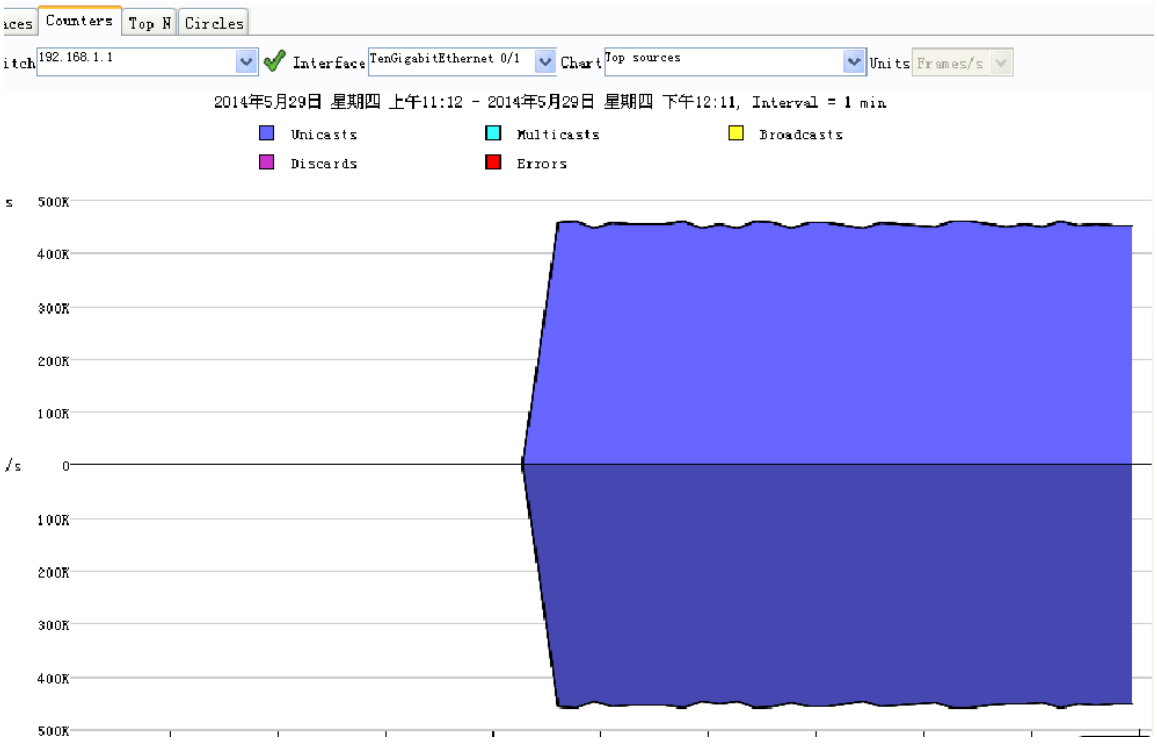


Figure 1-5 Counter Sampling Results



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
```

Third-Party Interfaces Configuration

1. Configuring Python

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*]]

Information Collection and Diagnostics Configuration

1. Configuring Tech-Support
2. Configuring HotKeys
3. Configuring Network Connectivity Test
4. Configuring Cluster Packet Tracing
5. Configuring Alarm and Event Management
6. Configuring the Function of Displaying Device Restart Reasons
7. Configuring Interface Link Diagnostics

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 2

1.2.1 Overview 2

1.2.2 Restrictions and Guidelines 2

1.2.3 Procedure 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

During the running process of the device, all the files required (such as configuration files and system software) are stored in the storage media of the device. Each storage medium supported by the device is called a file system **USB:**, **Flash:**, or **Tmp:**. The storage medium of the USB drive type is called **USB:**; the storage medium of the flash type is called **Flash:**; the storage medium of the Tmp type is called **Tmp:**.

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 in debug support mode to view the CLI commands that cause the fault, and collect the related fault information and save it in the **diag-info.txt** file 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.

```
Device# 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.

```
Device# debug support
Device(support)# execute diagnose-cmd copy xxx/xxx/xxx/core-xxx-xxx /data
This operation will modify file? [Y/N]:y
Device(support)# exit
Device# 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

(2) Enter the debug support mode.

debug support

(3) 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.

Contents

1 Configuring Hotkeys 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Restrictions and Guidelines 2

1 Configuring Hotkeys

1.1 Introduction

1.1.1 Overview

Hotkeys provide a method of device debugging and maintenance. When the device is abnormal or cannot be controlled, the network administrator can use hotkeys to view the memory information, interrupt information, lock occupancy and process information of the device. You can also use hotkeys to perform one-click collection, enable and disable the logging function of the console, obtain key debugging information of the device, locate the causes of the device errors, and restore the normal operation of the device.

1.1.2 Principles

Currently supported hotkeys include 4@ key combination and 4$ key combination. For details about the key combination, see *Hotkey Commands*.

Note

Hotkeys only support input in the serial terminal of the device, other types of terminals cannot take effect.

1. 4@ Key Combination

Note

4@ key combination can also be replaced with 4Esc (that is, press the **Esc** key on the keyboard 4 times continuously), and then press the relevant character or number keys.

4@ key combination means that you can press the @ key on the keyboard 4 times continuously, and then press the relevant character keys. The characters represent the following functions:

- **b**: restarts the device.
- **c**: starts and stops the console.
- **d**: displays occupation information of all locks.
- **h**: displays hotkey help information.
- **i**: displays CLI debugging information.
- **j**: displays interrupt information.
- **l**: displays the started process information.
- **m**: displays memory statistics of the device.
- **n**: enables periodic output of interrupt information.
- **o**: disables periodic output of interrupt information.
- **p**: disables the console from outputting logs.
- **q**: displays the context switch time and running time of all threads.

- **r**: displays the current stack information of all CPU cores.
- **s**: displays the status of all threads.
- **t**: displays the kernel stack information of all threads.
- **x**: enables the console to output dots.
- **y**: disables the console from outputting dots.

2. 4$ Key Combination

4$ key combination means that you can press the **$** key on the keyboard 4 times continuously, and then press the relevant character or number keys. The characters or numbers represent the following functions:

- 0-9: sets the log output level of the kernel.
- **b**: restarts the device.
- **c**: constructs abnormal crash of the system.
- **d**: prints all lock information of the kernel.
- **e**: uses SIGTERM to kill all processes.
- **f**: actively triggers Out Of Memory (OOM) to kill a low-priority process.
- **i**: uses SIGKILL to kill all processes.
- **j**: unfreezes the file system forcibly.
- **k**: shuts down the process that uses the current Teletypes (TTY).
- **h**: displays system hotkey help information.
- **l**: displays the active CPU stack information.
- **m**: displays memory information of the device.
- **n**: configures the real-time process as a common process.
- **o**: shuts down the system.
- **p**: displays register information of the device.
- **q**: displays timer information of the device.
- **r**: restores the keyboard mode to character mode.
- **s**: synchronizes the files in cache to the disk.
- **t**: displays the kernel stack information of all threads.
- **u**: mounts all file systems in read-only mode.
- **w**: displays the blocked thread information on the device.
- **z**: prints the Function Tracer (Ftrace) cache information.

1.2 Restrictions and Guidelines

- Only serial port terminals support the hotkeys, but other remote terminals (such as Telnet and SSH) do not support the hotkeys.

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.

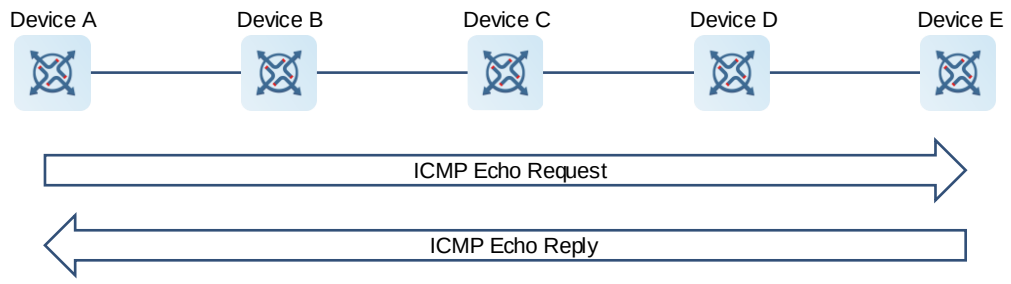
1.1.2 Principles

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.

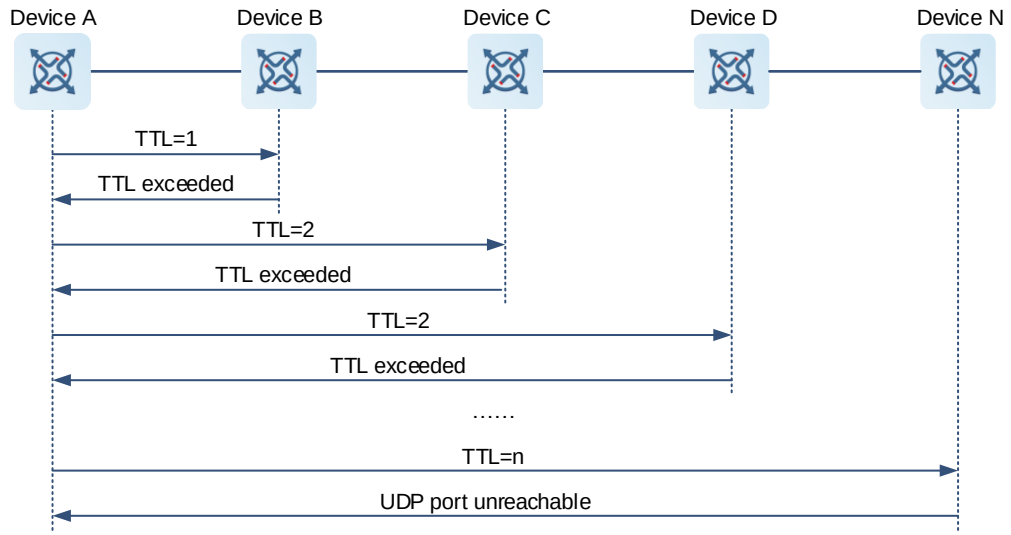
Figure 1-1 Testing Connectivity with Ping



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

- RFC 792: Internet Control Message Protocol
- RFC 4443: 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 user EXEC mode.

(2) Test whether the IP address is reachable.

(IPv4 network)

ping [**ip** | **vrf** *vrf-name*] { *hostname* | *ipv4-address* }

(IPv6 network)

ping [**ipv6** | **vrf** *vrf-name*] { *hostname* | *ipv6-address* }

By default, five 100-byte packets are sent to the specified IP address within two seconds.

(3) Enter the privileged EXEC mode.

enable

(4) Test 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*] | **save** *file-name* | **source** [*interface-type interface-number* | *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*] | **save** *file-name* | **source** [*interface-type interface-number* | *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 user EXEC mode.

(2) Configure the device to trace IP packets.

(IPv4 network)

traceroute [**ip** | **vrf** *vrf-name*] { *hostname* | *ipv4-address* }

(IPv6 network)

traceroute [**ipv6** | **vrf** *vrf-name*] { *hostname* | *ipv6-address* }

By default, the timeout time is 3 seconds, the number of probe packets to be sent is 3, the minimum TTL is 1, and the maximum TTL is 255.

(3) Enter the privileged EXEC mode.

enable

(4) Configure the device to trace IP packets.

(IPv4 network)

traceroute [**ip** | **vrf** *vrf-name*] { *hostname* | ipv4-*address* } [**out-interface** *interface-type interface-number* [**next-hop** *next-hop*] | **probe** *probe* | **save** *file-name* | **source** [*interface-type interface-number* | *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* | **save** *file-name* | **source** [*interface-type interface-number* | *source-ipv6-address*] | **timeout** *time* | **ttl** *minimum maximum*] *

By default, the timeout time is 3 seconds, the number of probe packets to be sent is 3, the minimum TTL is 1, and the maximum TTL is 255.

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

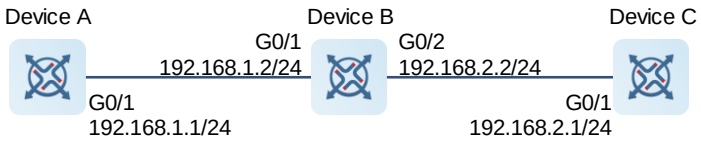
1.7.1 Configuring a Ping Connectivity Test

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 Topology for 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 10, 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.

```
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
```

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.

```
DeviceA# ping 192.168.2.1 length 1500 ntimes 10 data ffff source 192.168.1.1 timeout
3
Sending 10, 1500-byte ICMP Echoes to 192.168.2.1, timeout is 3 seconds:
< press Ctrl+C to break >
!!!!!!!!!!
Success rate is 10 percent (10/10), round-trip min/avg/max = 2/2/3 ms
```

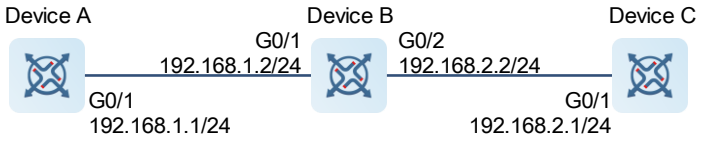
1.7.2 Configuring a Traceroute Connectivity Test

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 Topology for 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 Cluster Packet Tracing 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Principles 1

1.2 Monitoring 1

1 Configuring Cluster Packet Tracing

1.1 Introduction

1.1.1 Overview

Cluster packet tracking includes a comprehensive set of mechanisms for packet tracing within a cluster. By configuring matching conditions for target packets and running the **display** command, you can trace the flow of target packets in a cluster and identify packet loss locations and causes through fault symptom analysis. Cluster packet tracking enhances problem localization efficiency and simplify fault location.

1.1.2 Principles

During packet processing, the cluster monitors packets based on the configured packet matching rules. The information monitored by the cluster includes the nodes traversed by packets, number of packets, and packet delays at each node. Ultimately, the cluster packet tracing component collects the monitoring results and outputs them on the Command Line Interface (CLI). This function is typically used by developers to locate faults, such as packet loss and delay in a cluster.

1.2 Monitoring

Run the **show** command to check the configuration.

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

Table 1-1 Monitoring

Command	Purpose
clear pkt configure	Clears the configured packet matching rules.
clear pkt statistic	Clears the packet matching results and restarts counting.
show pkt configure	Displays the configured packet matching rules.
show pkt statistic	Displays the packet matching results.

Contents

1 Configuring Alarm and Event Management 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 Alarm Masking 2
1.4.1 Overview 2
1.4.2 Restrictions and Guidelines 2
1.4.3 Procedure 2
1.5 Configuring Alarm Suppression 2
1.5.1 Overview 2
1.5.2 Procedure 3
1.6 Monitoring 3
1.7 Configuration Examples 4
1.7.1 Configuring Alarm and Event Management 4

1 Configuring Alarm and Event Management

1.1 Introduction

1.1.1 Overview

Network device faults cause exceptions of services. When a fault occurs, you need to locate the fault quickly and troubleshoot it. An alarm is a notification generated by a device when a fault is detected. Checking an alarm with fault information is one of the most effective ways to locate the fault.

As the network grows in size and complexity, the failure of a service module may cause a large number of alarms. If all alarms are sent to the network management server or recorded and output through Syslog, system resources will be consumed and effective fault information cannot be collected.

You can manage the statistics and reports of alarms and events by the alarm management function. The alarms will be more effective and accurate, which helps a network manager to locate and troubleshoot faults efficiently.

- The alarm masking function masks alarms that users are not interested in to help them quickly obtain valuable fault information.
- The alarm suppression function controls the number of flapping alarms reported within a short period of time, and filters unstable alarms, to ensure that the user receives effective alarm information.

1.1.2 Principles

1. Basic Concepts

- Active Alarm

  An active indicates a persistent alarm. The active alarm persists if the fault is not fixed. When a service module detects a fault, it will send a notification to the alarm management module to inform the fault. The notification is displayed as an active alarm on the device.

- Historical Alarm

  Historical alarms record resolved alarms for fault location.

  When the service module reports the information about a resolved alarm, the alarm management module deletes the corresponding active alarm, records the recovery time, creates a historical alarm record, and updates the count and serial number of alarms. If the number of historical alarm records reaches the upper limit, the alarm management module deletes the earliest historical alarm record from the database.

- Event

  When an object or a status changes on the device, the notification generated by the device is called an event. Different from a persistent alarm, an event only displays a current change.

2. Active Alarm Report

If the service module reports that an active alarm is generated, the alarm management module checks the database to confirm the alarm. If the active alarm exists, the alarm management module does not handle the alarm notification. If the alarm does not exist, the alarm management module confirms whether the number of active alarms on the device reaches the upper limit. If the number of active alarms does not reach the upper

limit, the alarm management module sends the alarm to the network management server, or records and outputs the alarm through Syslog. If not, the alarm management module discards the alarm and records the alarm information in an internal log.

1.2 Restrictions and Guidelines

- Clearing current alarms or events manually using the **clear** command will not trigger a trap or any other messages.

1.3 Configuration Task Summary

The configuration tasks of alarm and event management are as follows. The following configuration tasks are optional. Select the configuration tasks as required.

- Configuring Alarm Masking
- Configuring Alarm Suppression

1.4 Configuring Alarm Masking

1.4.1 Overview

Redundant alarms make it difficult for users or O&M personnel to locate faults. You can configure the alarm masking function to mask the alarms that users are not interested in.

1.4.2 Restrictions and Guidelines

- You can configure different types of alarm masking rules. An alarm is masked when it matches one of the rules.
- If you cancel the masking for a specified alarm, the service module can report the alarm only when the alarm matches no masking rules.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the alarm masking function and configure masking rules.

alarm mask { **alarm-name** *alarm-name* | **all** | **slot** *slot-id* | **type** *alarm-type* }

The alarm masking function is disabled by default.

1.5 Configuring Alarm Suppression

1.5.1 Overview

For some service modules, the underlying state fluctuates frequently, which causes the alarm state to flap between alarm and recovery repeatedly within a short period of time. The alarm is not resolved during flapping.

The actual state is unstable. In this case, if each alarm or alarm clearance is reported, the alarm notifications may flood, which affects user experience.

The alarm suppression function suppresses the report of flapping alarms. The service module does not report two alarm records with the same source during suppression, to improve the accuracy of alarms.

For the alarms that cannot be ignored in the application scenario, you can disable the alarm suppression function to obtain all alarms.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable the alarm suppression function.

alarm jitter suppress disable

The alarm suppression function is enabled by default.

1.6 Monitoring

Run the **show** command to display the configuration.

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

Caution

During device operation, running the **clear** command may cause service interruption due to key information loss.

Table 1-1 Monitoring

Command	Purpose
clear alarm { **active** | **history** } [**sequence-number** *alarm-number*]	Clears alarm information.
clear alarm statistic	Clears all alarm statistics.
clear event { **all** | **sequence-number** *event-number* }	Clears event information.
show alarm active [**alarm-name** *alarm-name* | **slot** *slot-id* | **type** *alarm-type*] [**all**]	Displays the information about active alarms.
show alarm config	Displays the global configuration of the alarm module.
show alarm config alarm-name *alarm-name*	Display the configuration of the a specified alarm.
show alarm config list	Displays the information about all alarms.

Command	Purpose
show alarm history [**alarm-name** *alarm-name* | **slot** *slot-id* | **type** *alarm-type*]	Displays the information about historical alarms.
show alarm mask [**alarm-name** *alarm-name* | **slot** *slot-id* | **type** *alarm-type*] [**all**]	Displays the information about masked alarms.
show alarm statistic [**alarm-name** *alarm-name* **slot** *slot-id*]	Displays the statistics of the alarm modules.
show event { **all** | **event-name** *event-name* | **slot** *slot-id* | **type** *event-type* }	Displays the information about events.

1.7 Configuration Examples

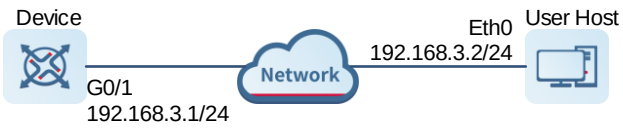
1.7.1 Configuring Alarm and Event Management

1. Requirements

The alarm and event management function enables the network administrator to obtain valid fault information of the device in a timely manner and efficiently locate the device fault.

2. Topology

Figure 1-1 Topology of Alarm and Event Management



3. Note

- Enable the alarm masking function.
- Enable the alarm suppression function when the function is disabled.

4. Procedure

(1) Enable the alarm masking function and specify masking rules.

```
Device> enable
Device# configure terminal
Device(config)# alarm mask alarm-name AsicFabricProtocalError
Device(config)# alarm mask slot 0
Device(config)# alarm mask type bus
```

(2) Enable the alarm suppression function.

```
Device> enable
DeviceA# configure terminal
```

```
Device(config)# no alarm jitter suppress disable
```

5. Verification

Run the **show alarm config**commandto display the global configuration of the alarm module.

```
Device# show alarm config
Alarm state    : ALL READY
Mask flag      : enable
Active count   : 65536
History count  : 2000
Event count    : 0
Mask config set : 0
Active sequence num  : 65536
History sequence num : 65542
Event sequence num   : 0
Old master nodeid    : 0
Slot exist flag     : 0x40000000 (dev1) 0x40000000 (dev2)
Slot online flag    : 0x40000000 (dev1) 0x40000000 (dev2)
Slot mask flag      : 0x40000000 (dev1)
Type mask flag      : 0x8000 0x0 0x0 0x0
Jitter suppress flag : enable
```

6. Configuration Files

- The configuration file of the device

```
!
alarm mask alarm-name AsicFabricProtocalError
alarm mask slot 0
alarm mask type bus
!
```

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 the self-healing mode of killing the target process or restarting the line card can ensure system availability, it also brings certain risks since such self-healing behaviors cannot be tracked and controlled uniformly. When a process is killed or a line card is restarted, it is difficult to locate the service that triggers the event. Once the logic of a detection service fails, the process is frequently killed or the line card is frequently restarted, which may cause more serious system exceptions. To address this issue, a component is required to track and control the self-healing of services. Level-2 Protect and Self-healing (PSH) provides a method of viewing the device restart cause on the CLI. When a device restarts, you can view the device restart reasons by using the command provided by the PSH module on 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.
show psh selfhealing	Displays system logs recorded by the PSH module.

Contents

1 Configuring Interface Link Diagnostics 1

1.1 Introduction 1

1.1.1 Overview 1

1.1.2 Working Principle 1

1.2 Monitoring 1

1 Configuring Interface Link Diagnostics

1.1 Introduction

1.1.1 Overview

Linklayer Service Module (LSM) process is a physical link layer service module. Interface link diagnosis organizes and maintains interface information through the LSM and provides other modules with the services of querying interface information and notifying interface events. The LSM collects and displays details of interface information, data source registration information, client registration information, and MOM database status for fault locating.

1.1.2 Working Principle

- When the interface status or configuration changes, the interface table information is updated. You can run the **show lsm interface** command to display all information about the current interface.
- When the LSM process starts, it obtains the capability values supported by the device. You can determine whether a function is supported by running the **show lsm capacity** command to display the capability values related to the interface.
- When the LSM process starts, other services register as the LSM client and monitor events related to the interface. Run the **show lsm client** command to display interface events that are monitored by each client. This is to determine whether to send the interface event to the client when the interface information changes.
- The LSM sends messages to other services through the MOM database. Run the **show lsm mom** command to display the messages that are sent.

1.2 Monitoring

Run the **show** command to check the configuration.

Run the **clear** command to clear statistics.

Table 1-1 Monitoring

Command	Purpose
show lsm apinfo [*ap-number*]	Displays information about LSM aggregate interfaces.
show lsm capacity	Displays information about LSM capability values.
show lsm client [**detail** | **pid** *client-pid*]	Displays information about LSM clients.
show lsm database [**data-source** | **interface**]	Displays information about the LSM internal database.
show lsm data-source	Displays information about the LSM data source.
show lsm debug-performance	Displays debugging information about LSM performance.

Command	Purpose
show lsm demux	Displays information about hyper-converged ports.
show lsm hook	Displays registration information about LSM preprocessing.
show lsm interface [*interface-index* | *interface-type interface-number*]	Displays details of LSM interfaces.
show lsm kernel [**apinfo** [*ap-number*] | **hook** | **interface** [*interface-index* | *interface-type interface-number*] [**statistic**] | **memory** | **timer** | **vrf**]	Displays information about the LSM kernel.
show lsm lib pid *pid* [**apinfo** [*ap-number*] | **hook** | **interface** [*interface-index* | *interface-type interface-number*] [**statistic**] | **memory** | **timer** | **vrf**]	Displays information about the LSM library.
show lsm linux	Displays native Linux messages configured by using the LSM.
show lsm memory	Displays information about LSM memory usage.
show lsm mom { **app_db** | **local_db** | **tunner_db** } [**cap_agg_global** | **cap_eth_glb** | **cap_ethif** | **cap_ifportrange** | **cap_stormctrl** | **data_agg_global** | **data_agg_intf** | **data_agg_mbr** | **data_ether_global** | **data_ether_drv** | **data_ethif** | **data_fiber_conf** | **data_if_counters** | **data_ifname_map** | **data_intf** | **data_stormctrl** | **dev_port** | **dev_port_static** | **fiber_state** | **port_det_result** | **ras_dsoverevt** | **state_agg_global** | **state_eth_split** | **state_ethif** | **state_fiber_info** | **state_fiber_oper** | **state_ifattri** | **state_ifcreate** | **state_intf** | **state_intflimit** | **task_eee** | **task_fiber** | **task_line_detect**] [*interface-type interface-number* | *db-index*]	Displays information about the LSM MOM database.
show lsm mom sub-counts	Displays the number of database subscriptions.
show lsm net-client	Displays information about LSM NET client events.
show lsm redundancy	Displays information about LSM hot standby.
show lsm rpc_agent	Displays information about the LSM RPC proxy.

Command	Purpose
show lsm split_cache_info	Displays information about LSM split interfaces.
show lsm timer	Displays information about the LSM timer.
show lsm troubleshooting	Displays information about LSM diagnosis.
show lsm vrf	Displays information about LSM VRF.
clear lsm redundancy statistics	Clears LSM hot standby statistics.