Ruijie RG-S2915-L Series Switches

S2915-L_RGOS 11.4(1)B82P4

Configuration Guide

Document Version: V1.3
Date: April 22, 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.ruijienetworks.com/
- Online support center: https://ruijienetworks.com/support
- Case portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Email support: service_rj@ruijienetworks.com
- Live chat: https://www.ruijienetworks.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.

Convention	Description
//	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.

System Configuration

1. Configuring CLI
2. Configuring Basic Management
3. Configuring Lines
4. Configuring Time Range
5. Configuring HTTP Service
6. Configuring Syslog
7. Configuring Security Logs
8. Configuring CWMP
9. Configuring MONITOR
10. Configuring ZAM
11. Configuring Supervisor Module Redundancy
12. Configuring PoE
13. Configuring Package Management
14. Configuring SF-APP
15. Configuring HOTKEY

1 Configuring CLI

1.1 Overview

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

Protocols and Standards

N/A

1.2 Applications

Application	Description
Configuring and Managing Network Devices Through CLI	You can enter commands in the CLI window to configure and manage network devices

1.2.1 Configuring and Managing Network Devices Through CLI

Scenario

As shown in Figure 1-1, a user accesses network device A using a PC, and enter commands in the CLI window to configure and manage the network device.

Figure 1-1

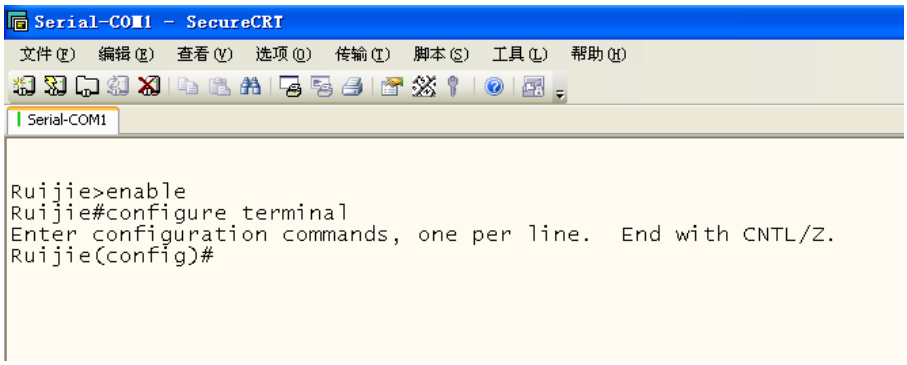


Remarks	A is the network device to be managed. PC is a terminal.

Deployment

As shown in Figure 1-2, the user uses the Secure CRT installed on a PC to set up a connection with network device A, and opens the CLI window to enter configuration commands.

Figure 1-2



1.3 Features

Overview

Feature	Description
Accessing CLI	You can log in to a network device for configuration and management.
Command Modes	The CLI provides several command modes. Commands that can be used vary according to command modes.
System Help	You can obtain the help information of the system during CLI configuration.
Abbreviated Commands	If the entered string is sufficient to identify a unique command, you do not need to enter the full string of the command.
No and Default Options of Commands	You can use the **no** option of a command to disable a function or perform the operation opposite to the command, or use the **default** option of the command to restore default settings.
Prompts Indicating Incorrect Commands	An error prompt will be displayed if an incorrect command is entered.
History Commands	You can use short-cut keys to display or call history commands.
Featured Editing	The system provides short-cut keys for editing commands.
Searching and Filtering of the Show Command Output	You can run the **show** command to search or filter specified commands.
Command Alias	You can configure alias of a command to replace the command.

1.3.1 Accessing CLI

Before using the CLI, you need to connect a terminal or PC to a network device. You can use the CLI after starting the network device and finishing hardware and software initialization. When used for the first time, the network device can be connected only through the console port, which is called out band management. After performing relevant configuration, you can connect and manage the network device through Telnet.

1.3.2 Command Modes

Due to the large number of commands, these commands are classified by function to facilitate the use of commands. The CLI provides several commands modes, and all commands are registered in one or several command modes. You must first enter the command mode of a command before using this command. Different command modes are related with each other while distinguished from each other.

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

To use more commands, you must first 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 of a certain configuration mode (such as global configuration mode and interface configuration mode) will affect configuration in use. If you save the configuration, these commands will be saved and executed next time the system is restarted. You must enter global configuration mode before entering another configuration mode, such as interface configuration mode.

The following table summarizes the command modes by assuming that the name of the network device is "Hostname".

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
User EXEC (User EXEC mode)	Enter User EXEC mode by default when accessing a network device.	Hostname>	Run the **exit** command to exit User EXEC mode. Run the **enable** command to enter Privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC (Privileged EXEC mode)	In User EXEC mode, run the **enable** command to enter Privileged EXEC mode.	Hostname#	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 configuration takes effect. This mode is password protected.

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
Global configuration (Global configuration mode)	In Privileged EXEC mode, run the **configure** command to enter global configuration mode.	Hostname(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. When using the **interface** command, you must specify the interface. Run the **vlan** *vlan_id* command to enter VLAN configuration mode.	Using commands in this mode will affect the global parameters of the network device.
Interface configuration (Interface configuration mode)	In global configuration mode, run the **interface** command to enter interface configuration mode.	Hostname(config-if)#	Run the **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **exit** command to return to global configuration mode. When using the **interface** command, you must specify the interface.	Use this configuration 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.	Hostname(config-vlan)#	Run the **end** command, or press **Ctrl+C** to return to the Privileged EXEC mode. Run the **exit** command to return to global configuration mode.	Use this configuration mode to configure VLAN parameters.

1.3.3 System Help

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

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

For example

```
Hostname>?

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.

For example

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

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

```
Hostname(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.

For example

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

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

For example

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

In any command mode, run the **help** command to obtain brief description about the help system.

For example

```
Hostname(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?'.)
```

1.3.4 Abbreviated Commands

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

For example, to run the **interface** *gigabitEthernet 0/1* command in GigabitEthernet 0/1 interface configuration mode, enter the abbreviated command as follows:

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

1.3.5 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 the operation opposite to the command. For example, run the **no shutdown** command to perform the operation opposite to the **shutdown** command, that is, enabling 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 default settings of the command. Default values of most commands are used to disable related functions. Therefore, the function of the **default** option is the same as that of the **no** option in most cases. For some commands, however, the default values are used to enable related functions. 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 related function and set the variables to default values.

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

1.3.6 Prompts Indicating Incorrect Commands

When you enter an incorrect command, an error prompt is displayed.

The following table lists the common CLI error messages.

Error Message	Meaning	How to Obtain Help
% Ambiguous command: "show c"	The characters entered are insufficient for identifying a unique command.	Re-enter the command, and enter a question mark after the word that is ambiguous. All the possible keywords will be displayed.
% Incomplete command.	The mandatory keyword or variable is not entered in the command.	Re-enter the command, and enter a space and a question mark. All the possible keywords or variables will be displayed.
% Invalid input detected at '^' marker.	An incorrect command is entered. The sign (^) indicates the position of the word that causes the error.	At the current command mode prompt, enter a question mark. All the command keywords allowed in this command mode will be displayed.

1.3.7 History Commands

The system automatically saves commands that are entered recently. You can use short-cut keys to display or call history commands.

The methods are described in the following table.

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

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

1.3.8 Featured Editing

When editing the command line, you can use the keys or short-cut keys listed in the following table:

Function	Key or Short-Cut Key	Description
Move the cursor on the	Left key or Ctrl+B	Move the cursor to the previous character.

Function	Key or Short-Cut Key	Description
editing line.	Right key or Ctrl+B	Move the cursor to the next character.
	Ctrl+A	Move the cursor to the head of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete an entered character.	Backspace key	Delete one character to the left of the cursor.
	Delete key	Delete one character to the right of the cursor.
Move the output by one line or one page.	Return key	When displaying contents, press the **Return** key to move the output one line upward and display the next line. This operation is performed when the output does not end yet.
	Space key	When displaying contents, press the **Space** key to page down and display the next page. This operation is performed when the output does not end yet.

When the editing cursor is close to the right boundary, the entire command line will move to the left by 20 characters, and the hidden front part is replaced by the dollar ($) signs. You can use the related keys or short-cut keys to move the cursor to the characters in the front or return to the head of the command line.

For example, the whole **access-list** may exceed the screen width. When the cursor is close to the end of the command line for the first time, the entire command line moves to the left by 20 characters, and the hidden front part is replaced by the dollar signs ($). 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 by the dollar signs ($).

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

The default screen width is 80 characters.

1.3.9 Searching and Filtering of the Show Command Output

To search specified contents from the output of the **show** command, run the following command:

Command	Description
show *any-command* | **begin** *regular-expression*	Searches specified contents from the output of the **show** command. The first line containing the contents and all information that follows this line will be output.

The **show** command can be executed in any mode.

Searched contents are case sensitive.

To filter specified contents from the output of the **show** command, run the following commands:

Command	Description
show *any-command* | **exclude** *regular-expression*	Filters the output of the **show** command. Except those containing the specified contents, all lines will be output.
show *any-command* | **include** *regular-expression*	Filters the output of the **show** command. Only the lines containing the specified contents will be output.

To search or filter the output of the **show** command, you must enter a vertical line (|). After the vertical line, select the searching or filtering rules and contents (character or string). Searched and filtered contents are case sensitive.

```
Hostname#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
```

1.3.10 Command Alias

You can configure any word as the alias of a command to simplythe command input.

Configuration Effect

1. Replace a command with a word.

For example, configure "mygateway" as the alias of the **ip route** *0.0.0.0 0.0.0.0192.1.1.1* command. To run this command, you only need to enter "mygateway".

Replace the front part of a command with a word, and enter the later part.

For example, configure "ia" as the alias of the **ip address** command. To run this command, you need to enter "ia" and then the specified IP address and subnet mask.

Configuration Steps

↘ Displaying Default Alias

In User EXEC or Privileged EXEC mode, default alias are available for some commands. You can run the **show aliases** command to displaythese default aliases.

```
Hostname(config)#show aliases
Exec mode alias:
```

```
h                   help
p                   ping
s                   show
u                   undebug
un                  undebug
```

These default aliases cannot be deleted.

Configuring a Command Alias

Command	**alias** *mode command-alias original-command*
Parameter Description	*mode*: indicates the command mode of the command represented by the alias. *command-alias*: indicates the command alias. *original-command*: indicates the command represented by the alias.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, run the **alias** ? command to list all command modes that can be configured with aliases.

Displaying Settings of Command Aliases

Run the **show aliases** command to display alias settings in the system.

Notes

- The command replaced by an alias must start from the first character of the command line.
- The command replaced by an alias must be complete.
- The entire alias must be entered when the alias is used; otherwise, the alias cannot be identified.

Configuration Example

Defining an Alias to Replace the Entire Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the default route configuration command **ip route** *0.0.0.0 0.0.0.0 192.168.1.1*.
	`Hostname#configure terminal` `Hostname(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1`

Verification	● Run the **show alias** command to check whether the alias is configured successfully.
	`Hostname(config)#show alias`
	`Exec mode alias:`
	`  h  help`
	`  p  ping`

	s show u undebug un undebug Global configuration mode alias: ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
	● Use the configured alias to run the command, and run the **show running-config** command to check whether the alias is configured successfully.
	Hostname(config)#ir Hostname(config)#show running-config Building configuration... ! alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuring an alias ... ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" is entered !

Defining an Alias to Replace the Front Part of a Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the front part "**ip route**" of the default route configuration command.
	Hostname#configure terminal Hostname(config)#alias config ir ip route
Verification	● Run the **show alias** command to check whether the alias is configured successfully. Hostname(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias:

	ir ip route
	• Enter the alias "ir" and then the later part of the command "0.0.0.0 0.0.0.0 192.168.1.1". • Run the **show ap-config running** command to check whether the configuration is successful.
	Hostname(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1 Hostname(config)#show running Building configuration... ! alias config ir ip route //Configuring an alias ! ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" and the later part of the command are entered !

System Help

1. The system provides help information for command alias. An asterisk (*) will be displayed in front of an alias. The format is as follows:

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

For example, in Privileged EXEC mode, the default command alias "s" represents the **show** keyword. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
Hostname#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?", the keywords starting by "s" and alias information are displayed.

```
Hostname#s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

You can use the alias to obtain help information about the command represented by the alias.

For example, configure the alias "ia" to represent the **ip address** command in interface configuration mode. If you enter "ia?" in interface configuration mode, the help information on "ip address?" is displayed, and the alias is replaced by the command.

```
Hostname(config-if)#ia ?
```

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

If you enter a space in front of a command, the command represented by this alias will not be displayed.

2 Configuring Basic Management

2.1 Overview

This document is a getting started guide to network device management. It describes how to manage, monitor, and maintain network devices.

2.2 Applications

Application	Description
Network Device Management	A user logs in to a network device from a terminal and runs commands on a command line interface (CLI) to manage device configurations.

2.2.1 Network Device Management

Scenario

Network device management described in this document is performed through the CLI. A user logs in to Network Device A from a terminal and runs commands on the CLI to manage device configurations. See Figure 2-1.

Figure 2-1



2.3 Features

Basic Concepts

TFTP

Trivial File Transfer Protocol (TFTP) is a TCP/IP protocol which allows a client to transfer a file to a server or get a file from a server.

AAA

AAA is short for Authentication, Authorization and Accounting.

Authentication refers to the verification of user identities and the related network services.

Authorization refers to the granting of network services to users according to authentication results.

Accounting refers to the tracking of network service consumption by users. A billing system charges users based on consumption records.

AAA provides effective means of network management and security protection.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol at present.

Telnet

Telnet is a terminal emulation protocol in the TCP/IP protocol stack which provides access to a remote host through a virtual terminal connection. It is a standard protocol located at Layer 7 (application layer) of the Open System Interconnection (OSI) model and used on the internet for remote login. Telnet sets up a connection between the local PC and a remote host.

System Information

System information includes the system description, power-on time, 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 slot and module information. 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), and actual and maximum number of physical ports.

Overview

Feature	Description
User Access Control	Controls the terminal access to network devices on the internet based on passwords and privileges.
Login Authentication Control	Performs username-password authentication to grant access to network devices when AAA is enabled. (Authentication is performed by a dedicated server.)
Basic System Parameters	Refer to the parameters of a system, such as the clock, banner, and Console baud rate.
Displaying Configurations	Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the nonvolatile random access memory (NVRAM).
Multiple-configuration Booting	Allows users to modify the path for saving startup configurations of the device and the corresponding file name.
Zero Configuration	Allows automatic service delivery and configuration maintenance for remote devices after device power-on, without requiring manual operation of network administrators.
Telnet	Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.
Restart	Introduces system restart.
Running Batch File Commands	Runs the commands in batches.

2.3.1 User Access Control

User access control refers to the control of terminal access to network devices on the internet based on passwords and privileges.

Working Principle

Privilege Level

16 privilege levels are defined ranging from 0 to 15 for CLI on network devices to grant users access to different commands. Level 0 is the lowest level granting access to just a few commands, whereas level 15 is the highest level granting access to all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter global configuration mode by default). Levels 2–15 are privileged user levels with the device configuration permission.

Password Classification

Passwords are classified into two types: password and security. The first type refers to simple encrypted passwords at level 15. The second type refers to secure encrypted passwords at levels 0–15. If a level is configured with both simple and secure encrypted passwords, the simple encrypted password will not take effect. If you configure a non-15 level simple encrypted password, a warning is displayed and the password is automatically converted into a secure encrypted password. If you configure the same simple encrypted password and secure encrypted password at level 15, a warning is displayed.

Password Protection

Each privilege level on a network device has a password. An increase in privilege level requires the input of the target level password, whereas a reduction in privilege level does not require password input.

By default, only two privilege levels are password-protected, namely, level 1 (common user level) and level 15 (privileged user level). Sixteen privilege levels with password protection can be assigned to the commands in each mode to grant access to different commands.

If no password is configured for a privileged user level, access to this level does not require password input. You are advised to configure a password for security.

Command Authorization

Each command has its lowest execution level. A user with a privilege level lower than this level is not allowed to run the command. After the command is assigned a privilege level, users at this level and higher have access to the command.

Related Configuration

Configuring a Simple Encrypted Password

- Run the **enable password** command.

Configuring a Secure Encrypted Password

- Run the **enable secret** command.

- A secure encrypted password is used to control the switching between user levels. It has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

Configuring Command Privilege Levels

- Run the **privilege** command to assign a privilege level to a command.
- A command at a lower level is accessible by more users than a command at a higher level.

Raising/Lowering a User Privilege Level

- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.
- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.

Enabling Line Password Protection

- Line password protection is required for remote login (such as login through Telnet).
- Run the **password**[**0** | **7**] *line* command to configure a line password, and then run the **login** command to enable password protection.
- By default, terminals do not support the **lock** command.

2.3.2 Login Authentication Control

In login authentication with AAA disabled, the password entered by a user is checked against the configured line password. If they are consistent, the user can access the network device. In local authentication, 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 network device with proper management permissions.

In AAA, the username and password entered by a user are authenticated by a server. If authentication is successful, the user can access the network device and enjoy certain management permissions.

For example, a RADIUS server can be used to authenticate usernames and passwords and control users' management permissions on network devices. Network devices no longer store users' passwords, but send encrypted user information to the RADIUS server, including usernames, passwords, shared passwords, and access policies. This provides a convenient way to manage and control user access and improve user information security.

Working Principle

Line Password

If AAA is disabled, you can configure a line password used to verify user identities during login. After AAA is enabled, line password verification does not take effect.

Local Authentication

If AAA is disabled, you can configure local authentication to verify user identities and control management permissions by using the local user database. After AAA is enabled, local authentication does not take effect.

AAA

AAA provides three independent security functions, namely, Authentication, Authorization and Accounting. A server (or the local user database) is used to perform authentication based on the configured login authentication method list and control users' management permissions. For details about AAA, see *Configuring AAA*.

Related Configuration

Configuring Local User Information

- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.

Configuring Local Authentication for Line-Based Login

- Run the **login local** command (in the case that AAA is disabled).
- Perform this configuration on every device.

Configuring AAA Authentication for Line-Based Login

- The default authentication method is used after AAA is enabled.
- Run the **login authentication** command to configure a login authentication method list for a line.
- Perform this configuration when the local AAA authentication is required.

Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

- Run the **login access non-aaa** command in global configuration mode.
- Perform this configuration on every device.

Configuring the Connection Timeout Time

- The default connection timeout time is 10 minutes.
- Run the **exec-timeout** command to change the default connection timeout time. An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

Configuring the Session Timeout Time

- The default session timeout time is 0 minutes, indicating no timeout.
- Run the **session-timeout** command to change the default session timeout time.
- The session established to a remote host through a line will be disconnected if no output is detected during the timeout time. Then the remote host is restored to Idle. Perform this configuration when you need to increase or reduce the session timeout time.

Locking a Session

- By default, terminals do not support the **lock** command.
- Run the **lockable** command to lock the terminals connected to the current line.
- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command in terminal EXEC mode to lock the terminal.

2.3.3 Basic System Parameters

System Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour:minute:second, day of the week*.

When you use a network device for the first time, set its system clock to the current date and time manually.

Configuring a System Name and Command Prompt

You can configure a system name to identify a network device. The default system name is **Hostname**. A name with more than 32 characters will be truncated to keep only the first 32 characters. The command prompt keeps consistent with the system name.

Banner

A banner is used to display login prompt information. There are two types of banner: Daily notification and login banner.

- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.
- A login banner appears after daily notification to display login information.

Configuring the Console Baud Rate

You can manage network device through a Console port The first configuration on the network device must be performed through the Console port. The serial port baud rate can be changed based on actual requirements. Note that the management terminal must have consistent baud rate setting with the device console.

Configuring the Connection Timeout Time

The connection timeout time is used to control device connections (including established connections and sessions established to remote hosts). A connection will be closed when no input is detected during the timeout time.

Related Configuration

Configuring the System Date and Clock

- Run the **clock set** command to configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

Updating the Hardware Clock

- If the hardware clock and software clock are not synchronized, run the **clock update-calendar** command to copy the date and time of the software clock to the hardware clock.

Configuring a System Name

- Run the **hostname** command to change the default system name.
- The default host name is **Hostname**.

Configuring a Command Prompt

- Run the **prompt** command.

Configuring Daily Notification

- By default, no daily notification is configured.
- Run the **banner motd** command to configure daily notification.
- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.

Configuring a Login Banner

- By default, no login banner is configured.
- Run the **banner login** command to configure a login banner to display login information.

Configuring the Console Baud Rate

- Run the **speed** command.
- The default baud rate is 9,600 bps.

2.3.4 Displaying Configurations

Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the NVRAM.

Working Principle

Running Configurations

Running configurations, namely, running-config, are the configurations that individual component modules run in real time. A request can be made to all running components to collect configurations, which will be orchestrated before being displayed to users. Only running components may provide real-time configurations, whereas unloaded components do not display configurations. In the case that the system is started, and a component process is restarted, the configurations collected during this period may be inaccurate due to the component unstable state. For example, the configurations of a component may not be missing initially but can be displayed later.

Startup Configurations

The configurations stored in the NVRAM, namely, startup-config, are the configurations executed during device startup. When the system is restarted, startup-config is loaded to become new running-config. To display permanent configurations, the system needs to read the **startup-config** file in the NVRAM.

The startup-config file copied from external environment to the device only supports UTF-8(no BOM) format.

Related Configuration

Displaying Running Configurations

Run the **show running-config** [**interface** *interface*] command to display the configurations that the system is currently running or the configurations on an interface.

Displaying Startup Configurations

Run the **show startup-config** command.

Storing Startup Configurations

Run the **write** or **copy running-config startup-config** command to store the current running configurations as new startup configurations.

2.3.5 Multiple-configuration Booting

Multiple-configuration booting allows users to modify the path for saving startup configurations of the device and the corresponding file name. At present, configurations can be saved to an extended flash memory and an extended USB flash drive of a device. To save configurations in an extended USB flash drive, the device must support at least one USB interface. If the device supports two or more USB interfaces, startup configurations are saved in **/mnt/usb0**.

Working Principle

- By default, the startup configuration file of a device is saved in **Flash:/config.text** and named **config.text**. Use this command to modify the path for saving startup configurations of the device and the corresponding file name.

  The startup configuration file name follows a slash "/", for example, **flash:/Hostname.text**.

  The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **flash:/Hostname/Hostname.text** as an example, where the **flash:/Hostname** folder must exist. In master-slave mode, all device paths are required.

  To save the startup configuration file to a USB flash drive, the device must provide a USB interface with a USB flash drive inserted. Otherwise, configurations cannot be saved by using the **write** command. In master-slave mode, all devices must have USB flash drives connected.

Related Configuration

Modifying the Path for Saving Startup Configurations and the Corresponding File Name

Run the **boot config { flash:***filename* | **usb0:***filename* **}** command to modify the path for saving startup configurations and the corresponding file name.

Displaying the Path for Saving Startup Configurations and the Corresponding File Name

Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

2.3.6 Zero Configuration

The zero configuration function allows automatic service delivery and configuration maintenance for remote devices after device power-on, without requiring manual operation of network administrators.

Working Principle

The zero configuration function involves the following process: A device with default configurations is powered on, obtains a device management address from the DHCP server of the ACS, and sends the SNMP INFORM message to the ACS; after receiving the SNMP INFORM message, the ACS delivers startup configurations of the device, and immediately validates the configurations.

- The zero configuration function is applicable to the ACS solution only.
- The zero configuration function is applicable to standalone systems only.
- With the zero configuration function, DHCP Snooping Trust is enabled only on the last two electrical ports and all SFP ports of the device by default, regardless of whether the device supports the MGMT port.
- Enabling and disabling the zero configuration function will delete the startup configuration file of the device and trigger device restart.

Related Configuration

Enabling and Disabling the Zero Configuration Function

Run the **zcm** { **enable** | **disable** } command to enable or disable the zero configuration function.

2.3.7 Telnet

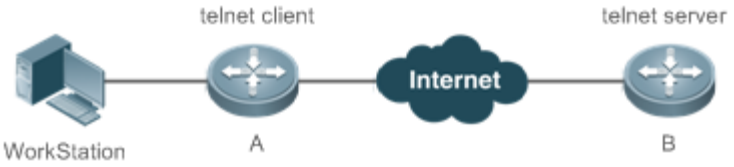
Working Principle

Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.

The Telnet Client service allows a local or remote user who has logged in to a network device to use its Telnet Client program to access other remote system resources on the internet. In Figure 2-2, a user with a PC connects to Network Device A by using the terminal emulation or Telnet program and then logs in to Network Device B by using the **telnet** command to perform configuration management.

Telnet program supports the use of IPv4 and IPv6 addresses. A Telnet server accepts Telnet connection requests that carry IPv4 and IPv6 addresses. A Telnet client can send connection requests to hosts identified by IPv4 and IPv6 addresses.

Figure 2-2



Related Configuration

Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

Restoring a Telnet Client Session

- Run the **<1-99>** command.

Disconnecting a Suspended Telnet Client Session

- Run the **disconnect** *session-id* command.

Enabling the Telnet Server Service

- Run the **enable service telnet-server** command.
- Perform this configuration when you need to enable Telnet login.

2.3.8 Restart

The timed restart feature makes user operation easier in some scenarios (such as tests).

- If you configure a time interval, the system will restart after the interval. The interval is in the format of *mmm* or *hhh:mm*, in the unit of minutes. You can specify the interval name to reflect the restart purpose.
- If you define a future time, the system will restart when the time is reached.

⚠ The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

⚠ The span between the restart time and current time must not exceed 31 days, and the restart time must be later than the current system time. After you configure a restart plan, do not to change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Configuration

Configuring Restart

- Run the **reload** command to configure a restart policy.
- Perform this configuration when you need to restart a device at a specific time.

2.3.9 Running Batch File Commands

In system management, sometimes it takes a long time to enter many commands on the CLI to manage a function. This process is prone to errors and omissions. You can put the commands to a batch file according to configuration steps and execute the file to complete related configuration.

You can specify the name and content of the batch file on your PC and transfer the file to the device flash memory through TFTP. The batch processing content simulates user input. Therefore, you need to edit the batch file content according to the CLI command configuration sequence. In addition, you need to write the responses to interactive commands to the batch file to ensure normal command execution.

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

Related Configuration

Batch-Running Commands

- Run **execute** to run the commands in batches.
- This command provides a convenient way to run multiple commands at a time.

2.4 Configuration

Configuring Passwords and Privileges	(Optional) It is used to configure passwords and command privilege levels.	
	enable password	Configures a simple encrypted password.
	enable secret	Configures a secure encrypted password.
	enable	Raises a user privilege level.
	disable	Lowers a user privilege level.
	privilege	Configures command privilege levels.
	password	Specifies a line password.
	login	Enables line password protection.
Configuring Login and Authentication	(Optional) It is used to configure different login modes and authentication methods.	
	username	Configures local user account information and optional authorization information.
	login local	Configures local authentication for line-based login.
	login access non-aaa	Configures non-AAA authentication for line-based login when AAA is enabled.
	login authentication	Configures AAA authentication for line-based login.
	telnet	Enables the Telnet Client service.

	do telnet	Enables the DoTelnet Client service.
	enable service telnet-server	Enables the Telnet Server service.
	exec-timeout	Configures the connection timeout time.
	session-timeout	Configures the session timeout time.
	lockable	Enables line-based terminal lock.
	lock	Locks a terminal connected to the current line.
Configuring Basic System Parameters	(Optional) It is used to configure basic system parameters.	
	clock set	Configures the system date and clock.
	clock update-calendar	Updates the hardware clock.
	hostname	Configures a system name.
	prompt	Configures a command prompt.
	banner motd	Configures daily notification.
	bannerlogin	Configures a login banner.
	speed	Configures the Console baud rate.
Enabling and Disabling a Specific Service	(Optional) It is used to enable and disable a specific service.	
	enable service	Enables a service.
Configuring Multiple-configuration Booting	(Optional) It is used to modify the startup configuration file.	
	boot config { flash:*filename* **| usb0:***filename* **}**	Modifies the path for saving startup configurations and the corresponding file name.
Configuring the Zero Configuration Function	(Optional) It is used to enable or disable the zero configuration function.	
	zcm { enable | disable }	Enables or disables the zero configuration function.
Configuring a Restart Policy	(Optional) It is used to configure a system restart policy.	
	reload	Restarts a device.
Running Batch File Commands	(Optional) It is used to run the commands in batches.	
	execute { [**flash:**] *filename* }	Runs the commands in batches.

2.4.1 Configuring Passwords and Privileges

Configuration Effect

- Configure passwords to control users' access to network devices.
- Assign a privilege level to a command to grant the command access to only the users at or higher than the level.

- Lower the command privilege level to grant more users access to the command.
- Raise the command privilege level to limit the command access to a few users.

Notes

- You can use the password configuration command with the **level** option to configure a password for a specific privilege level. After you specify the level and the password, the password works for the users who need to access this level.
- By default, no password is configured for any level. The default level is 15.
- If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password.
- The system chooses the secure encrypted password over the simple encrypted password if both of them are configured.

Configuration Steps

Configuring a Simple Encrypted Password

- (Optional) Perform this configuration when you need to establish simple encrypted password verification when users switch between different privilege levels.
- Run the **enable password** command to configure a simple encrypted password.

Configuring a Secure Encrypted Password

- (Optional) Perform this configuration when you need to establish secure encrypted password verification when users switch between different privilege levels.
- Run the **enable secret** command to configure a secure encrypted password.
- A secure encrypted password has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

Configuring Command Privilege Levels

- Optional.
- A command at a lower level is accessible by more users than a command at a higher level.

Raising/Lowering a User Privilege Level

- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.
- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.

Enabling Line Password Protection

- (Optional) Line password protection is required for remote login (such as login through Telnet).
- Run the **password** [**0** | **7**] *line* command to configure a line password, and then run the **login** command to enable login authentication.

If a line password is configured but login authentication is not configured, the system does not display password prompt.

Verification

- Run the **show privilege** command to display the current user level.
- Run the **show running-config** command to display the configuration.

Related Commands

Configuring a Simple Encrypted Password

Command	**enable password** [**level** *level*] { *password* | [**0** | **7**] *encrypted-password* }
Parameter Description	*level*: Indicates a specific user level. *password:* Indicates the password used to enter privileged EXEC mode. *0:* Indicates that the password is entered in plaintext. *7:* Indicates that the password is entered in cyphertext. *encrypted-password:* Indicates the password text, which must contain case-sensitive English letters and digits. Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.
Command Mode	Global configuration mode
Usage Guide	Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured. If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password. If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed. If you specify an encryption type and enter a password in plaintext, you cannot re-enter privileged EXEC mode. An encrypted password cannot be retrieved once lost. You have to configure a new password.

Configuring a Secure Encrypted Password

Command	**enable secret** [**level** *level*] {*secret* | [**0 | 5**] *encrypted-secret*}
Parameter Description	*level*: Indicates a specific user level. secret: Indicates the password used to enter privileged EXEC mode. **0 | 5**: Indicates the password encryption type. 0 indicates no encryption, and 5 indicates secure encryption. *encrypted-password*: Indicates the password text.
Command Mode	Global configuration mode

Usage Guide	Use this command to configure passwords for different privilege levels.

Raising a User Privilege Level

Command	**enable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	An increase in privilege level requires the input of the target level password.

Lowering a User Privilege Level

Command	**disable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	A reduction in privilege level does not require password input. Use this command to exit Privileged EXEC mode and return to user EXEC mode. If *privilege-level* is specified, the current privilege level is reduced to the specified level. *privilege-level* must be lower than the current level.

Configuring Command Privilege Levels

Command	**privilege** *mode* [**all**] { **level** *level* | **reset** } *command-string*
Parameter Description	*mode*: Indicates the CLI mode of the command. For example, **config** indicates the global configuration mode, **EXEC** indicates the privileged command mode, and **interface** indicates the interface configuration mode. **all**: Changes the subcommand privilege levels of a specific command to the same level. **level** *level*: Indicates a privilege level, ranging from 0 to 15. **reset**: Restores the command privilege level to the default. *command-string*: Indicates the command to be assigned a privilege level.
Command Mode	Global configuration mode
Usage Guide	To restore a command privilege level, run the **no privilege** *mode* [**all**] **level** *level command* command in global configuration mode.

Specifying a Line Password

Command	**password**[**0** | **7**] *line*
Parameter Description	**0**: Indicates to configure a password in plaintext. **7**: Indicates to configure a password in cyphertext. line: Indicates the password string.

Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Line Password Protection

Command	**login**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

Configuring Command Authorization

Scenario	Assign privilege level 1 to the **reload** command and its subcommands and configure level 1 as the valid level (by configuring the **test** password).
Configuration Steps	● Assign privilege level 1 to the **reload** command and its subcommands.

	`Hostname# configure terminal`
	`Hostname(config)# privilege exec all level 1 reload`
	`Hostname(config)# enable secret level 1 0 test`
	`Hostname(config)# end`

Verification	● Check whether the **reload** command and its subcommands are accessible at level 1.

	`Hostname# disable 1`
	`Hostname> reload ?`
	`at reload at<cr>`

2.4.2 Configuring Login and Authentication

Configuration Effect

- Establish line-based login identity authentication.
- Run the **telnet** command on a network device to log in to a remote device.
- Close an established connection if no output is detected during the timeout time.
- Disconnect an established session connecting to a remote host and restore the host to Idle if no output is detected during the timeout time.

- Lock a terminal to deny access. 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.

Configuration Steps

Configuring Local User Information

- Mandatory.
- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.
- Perform this configuration on every device.

Configuring Local Authentication for Line-Based Login

- Mandatory.
- Configure local authentication for line-based login in the case that AAA is disabled.
- Perform this configuration on every device.

Configuring AAA Authentication for Line-Based Login

- (Optional) Perform this configuration to configure AAA authentication for line-based login.
- Configure AAA authentication for line-based login in the case that AAA is enabled.
- Perform this configuration on every device.

Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

- Optional.
- Run the **login access non-aaa** command in global configuration mode to authenticate line-based login in non-AAA mode in the case that AAA is enabled.
- Perform this configuration on every device.

Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

Restoring a Telnet Client Connection

- (Optional) Perform this configuration to restore the connection on a Telnet client.

Closing a Suspended Telnet Client Connection

- (Optional) Perform this configuration to close the suspended connection on a Telnet client.

Enabling the Telnet Server Service

- Optional.
- Enable the Telnet Server service when you need to enable Telnet login.

Configuring the Connection Timeout Time

- Optional.
- An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

Configuring the Session Timeout Time

- Optional.
- The session connecting to a remote host will be disconnected and the host be restored to Idle if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the session timeout time.

Locking a Session

- (Optional) Perform this configuration when you need to temporarily exit a session on a device.
- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command to lock the terminal.

Verification

- Run the **show running-config** command to display the configuration.
- In the case that AAA is disabled, after local user information and line-based local authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- In the case that AAA is enabled, after local user information and local AAA authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- Run the **show user** command to display the information about the users who have logged in to the CLI.
- Telnet clients can connect to devices enabled with the Telnet Server service.
- When a user presses **Enter** on a locked CLI, the user is prompted for password input. The session is unlocked only when the entered password is the same as the configured one.
- Run the **show sessions** command to display every established Telnet client instance.

Related Commands

Configuring Local User Information

Command	**username** *name* [**login mode** { **aux** | **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string* | **secret** [**0** | **5**] *text-string*
Parameter Description	*name*: Indicates a user name. **login mode**: Indicates the login mode. **aux**: Sets the login mode to AUX. **console**: Sets the login mode to Console.

	ssh: Sets the login mode to SSH. **telnet**: Sets the login mode to Telnet. **online amount** *number*: Indicates the maximum number of online accounts. **permission** *oper-mode path*: Configures the file operation permission. *op-mode* indicates the operation mode, and *path* indicates the directory or path of a specific file. **privilege** *privilege-level*: Indicates the account privilege level, ranging from 0 to 15. **reject remote-login**: Rejects remote login by using the account. **web-auth**: Allows only Web authentication for the account. **pwd-modify**: Allows the account owner to change the password. This option is available only when **web-auth** is configured. **nopassword**: Indicates that no password is configured for the account. **password** [**0** | **7**] *text-string*: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 7 indicates that the password is input in cyphertext. The default is plaintext. **secret** [**0** | **5**] *text-string*: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 5 indicates that the password is input in cyphertext. The default is plaintext.
Command Mode	Global configuration mode
Usage Guide	Use this command to create a local user database to be used by authentication. If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters. This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.

Configuring Local Authentication for Line-Based Login

Command	**login local**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	Use this command to configure local authentication for line-based login in the case that AAA is disabled. Local user information is configured by using the **username** command.

Configuring AAA Authentication for Line-Based Login

Command	**login authentication** { **default** | *list-name* }
Parameter Description	**default:** Indicates the default authentication method list name. *list-name*: Indicates the optional method list name.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure AAA authentication for line-based login in the case that AAA is enabled. The AAA authentication methods, including RADIUS authentication, local authentication, and no authentication,

	are used during the authentication process.

Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

Command	**login access non-aaa**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command when you need to perform non-AAA authentication on line-based login in the case that AAA is enabled. The configuration takes effect for all terminals.

Enabling the Telnet Client Service

Command	**telnet** [**oob**] *host* [*port*] [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name* }] [**/vrf** *vrf-name*]
Parameter Description	**oob:** Remotely connects to a Telnet server through out-of-band communication (by using a management port). This option is available only when the device has a management port. *host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *port*: Indicates the TCP port number of the Telnet server. The default value is 23. **/source:** Indicates the source IP address or source port used by a Telnet client. **ip** *A.B.C.D:* Indicates the source IPv4 address used by the Telnet client. **ipv6** *X:X:X:X::X:* Indicates the source IPv6 address used by the Telnet client. **interface** *interface-name*: Indicates the source port used by the Telnet client. **/vrf** *vrf-name*: Indicates the name of the virtual routing and forwarding (VRF) table to be queried.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

Restoring a Telnet Client Session

Command	<1-99>
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	Use this command to restore a Telnet client session. A user can press the shortcut key **Ctrl**+**Shift**+**6 X** to temporarily exit the Telnet client session that is established using the **telnet** command, run the **<1-99>** command to restore the session, and run the **show sessions** command to display the session information.

Closing a Suspended Telnet Client Connection

Command	**disconnect** *session-id*
Parameter	*session-id*: Indicates the suspended Telnet client session ID.

Description	
Command Mode	User EXEC mode
Usage Guide	Use this command to close a specific Telnet client session by entering the session ID.

Enabling the Telnet Server Service

Command	**enable service telnet-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the Telnet Server service. The IPv4 and IPv6 services are also enabled after the command is executed.

Configuring the Connection Timeout Time

Command	**exec-timeout** *minutes* [*seconds*]
Parameter Description	*minutes*: Indicates the connection timeout time in the unit of minutes. *seconds*: Indicates the connection timeout time in the unit of seconds.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the established connections on a line. A connection will be closed when no input is detected during the timeout time. To remove the connection timeout configuration, run the **no exec-timeout** command in line configuration mode.

Configuring the Session Timeout Time

Command	**session-timeout** *minutes*[**output**]
Parameter Description	*minutes*: Indicates the session timeout time in the unit of minutes. **output**: Indicates whether to add data output as a timeout criterion.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the remote host sessions on a line. A session will be disconnected when no input is detected during the timeout time. To cancel the session timeout time, run the **no session-timeout** command in line configuration mode.

Enabling Line-Based Terminal Lock

Command	**lockable**
Parameter Description	N/A
Command Mode	Line configuration mode

Usage Guide	N/A

Locking a Terminal Connected to the Current Line

Command	**lock**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

Establishing a Telnet Session to a Remote Network Device

Configuration Steps	● Establish a Telnet session to a remote network device with the IP address 192.168.65.119. ● Establish a Telnet session to a remote network device with the IPv6 address 2AAA:BBBB::CCCC. ● Run the **telnet** command in privileged EXEC mode, and run the **do telnet** command in privileged EXEC mode/configuration mode/interface configuration mode.

	`Hostname# telnet 192.168.65.119`
	`Trying 192.168.65.119 ... Open`
	`User Access Verification`
	`Password:`

	`Hostname# telnet 2AAA:BBBB::CCCC`
	`Trying 2AAA:BBBB::CCCC ... Open`
	`User Access Verification`
	`Password:`

Verification	● Check whether the Telnet sessions are established to the remote network devices.

Configuring the Connection Timeout Time

Configuration Steps	● Set the connection timeout time to 20 minutes.

	`Hostname# configure terminal//Enter global configuration mode.`
	`Hostname# line vty 0 //Enter line configuration mode.`
	`Hostname(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.`

Verification	● Check whether the connection between a terminal and the local device is closed when no input is detected during the timeout time.

Configuring the Session Timeout Time

Configuration Steps	● Set the session timeout time to 20 minutes.

	Hostname# configure terminal//Enter global configuration mode.
	Hostname(config)# line vty 0 //Enter line configuration mode.
	Hostname(config-line)#session-timeout 20//Set the session timeout time to 20 minutes.

Verification	● Check whether the session between a terminal and the local device is disconnected when no input is detected during the timeout time.

2.4.3 Configuring Basic System Parameters

Configuration Effect

- Configure basic system parameters.

Configuration Steps

Configuring the System Date and Clock

- Mandatory.
- Configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

⚠ The time configuration is applied only to the software clock if the network device does not provide a hardware clock. The configuration will be invalid when the device is powered off.

Updating the Hardware Clock

- Optional.
- Perform this configuration when you need to copy the date and time of the software clock to the hardware clock so that the hardware clock is synchronized with the software clock.

Configuring a System Name

- (Optional) Perform this configuration to change the default system name.

Configuring a Command Prompt

- (Optional) Perform this configuration to change the default command prompt.

Configuring Daily Notification

- (Optional) Perform this configuration when you need to display important prompts or warnings to users.
- You can configure notification in one or multiple lines, which will be displayed to users after login.

Configuring a Login Banner

- (Optional) Perform this configuration when you need to display important messages to users upon login or logout.

Configuring the Console Baud Rate

- (Optional) Perform this configuration to change the default Console baud rate.

Verification

- Run the **show clock** command to display the system time.
- Check whether a login banner is displayed after login.
- Run the **show version** command to display the system information and version.

Related Commands

Configuring the System Date and Clock

Command	**clock set** *hh:mm:ss month day year*
Parameter Description	*hh:mm:ss*: Indicates the current time, in the format of *hour* (24-hour format):*minute*:*second*. *day*: Indicates a day (1–31) of the month. *month*: Indicates a month (from January to December) of the year. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to configure the system time. If the device does not provide a hardware clock, the time configuration will be invalid when the device is powered off.

Updating the Hardware Clock

Command	**clock update-calendar**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After the configuration, the time of the software clock will overwrite that of the hardware clock.

Configuring a System Name

Command	**hostname** *name*
Parameter Description	*name*: Indicates the system name, which must consist of printable characters and must not exceed 63 bytes.

Command Mode	Global configuration mode
Usage Guide	To restore the system name to the default, run the **no hostname** command in global configuration mode.

Configuring a Command Prompt

Command	**prompt** *string*
Parameter Description	*string*: Indicates the command prompt name. A name with more than 32 characters will be truncated to keep only the first 32 characters.
Command Mode	Privileged EXEC mode
Usage Guide	To restore the command prompt to the default settings, run the **no prompt** command in global configuration mode.

Configuring Daily Notification

Command	**banner motd** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes.

Configuring a Login Banner

Command	**banner login** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes. To remove the login banner configuration, run the **no banner login** command in global configuration mode.

Configuring the Console Baud Rate

Command	**speed** *speed*
Parameter Description	*speed*: Indicates the console baud rate, in the unit of bps. The serial port baud rate can be set to 9,600 bps, 19,200 bps, 38,400 bps, 57,600 bps, or 115,200 bps. The default is 9,600 bps.
Command Mode	Line configuration mode
Usage Guide	You can configure the asynchronous line baud rate based on requirements. The **speed** command is used to

	configure receive and transmit rates for the asynchronous line.

Configuration Example

Configuring the System Time

Configuration Steps	● Change the system time to 2003-6-20, 10:10:12.
	`Hostname# clock set 10:10:12 6 20 2003 //Configure the system time and date.`
Verification	● Run the **show clock** command in privileged EXEC mode to display the system time.
	`Hostname# show clock //Confirm that the changed system time takes effect.` `clock: 2003-6-20 10:10:54`

Configuring Daily Notification

Configuration Steps	● Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.

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

Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.

	`C:\>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:`

Configuring a Login Banner

Configuration Steps	● Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.

	Hostname(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#'. Access for authorized users only. Please enter your password. # //Ending delimiter Hostname(config)#
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether the login banner is displayed before the CLI appears.
	C:\>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:

Configuring the Serial Port Baud Rate

Configuration Steps	● Set the serial port baud rate to 57,600 bps.

	Hostname# configure terminal //Enter global configuration mode.
	Hostname(config)# line console 0 //Enter console line configuration mode.
	Hostname(config-line)# speed 57600 //Set the console baud rate to 57,600 bps.
	Hostname(config-line)# end //Returns to privileged mode.

Verification	● Run the **show** command to display the configuration.
	Hostname# show line console 0 //Displays the console configuration. 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

Configuration Steps	● Set the serial port baud rate to 57,600 bps.

	Hostname# configure terminal //Enter global configuration mode.
	Hostname(config)# line console 0 //Enter console line configuration mode.
	Hostname(config-line)# speed 57600 //Set the console baud rate to 57,600 bps.
	Hostname(config-line)# end //Returns to privileged mode.

Verification	● Run the **show** command to display the configuration.
	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

2.4.4 Enabling and Disabling a Specific Service

Configuration Effect

- Dynamically adjust system services when the system is running, and enable and disable specific services (SNMP Agent, SSH Server, and Telnet Server).

Configuration Steps

↘ **Enabling the SNMP Agent, SSH Server, and Telnet Server Services**

- (Optional) Perform this configuration when you need to use these services.

Verification

- Run the **show running-config** command to display the configuration.
- Run the **show services** command to display the service Enabled/Disable state.

Related Commands

↘ **Enabling the SSH Server, Telnet Server, and SNMP Agent Services**

Command	**enable service** { **ssh-server** | **telnet-server** | **snmp-agent** }
Parameter	**ssh-server:** Enables or disables the SSH Server service. The IPv4 and IPv6 services are also enabled

Description	together with this service. **telnet-server:** Enables or disables the Telnet Server service. The IPv4 and IPv6 services are also enabled together with this service. **snmp-agent:** Enables or disables the SNMP Agent service. The IPv4 and IPv6 services are also enabled together with this service.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable and disable specific services.

Configuration Example

Enabling the SSH Server Service

Configuration Steps	● Enable the SSH Server service.
	Hostname# configure terminal //Enter global configuration mode. Hostname(config)#enable service ssh-server //Enable the SSH Server service.
Verification	● Run the **show running-config** command to display the configuration. ● Run the **show ip ssh** command to display the configuration and running state of the SSH Server service.

2.4.5 Configuring Multiple-configuration Booting

Configuration Effect

- Modify the path for saving startup configurations and the corresponding file name.

Notes

- The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **`flash:/Hostname/Hostname.text`** as an example, where the **`flash:/Hostname`** folder must exist. In master-slave mode, all device paths are required.
- To save the startup configuration file to a USB flash drive, the device must provide a USB interface with a USB flash drive inserted. Otherwise, configurations cannot be saved by using the **write** command. In master-slave mode, all devices must have USB flash drives connected.

Configuration Steps

Modifying the Path for Saving Startup Configurations and the Corresponding File Name

- (Optional) Perform this configuration when you need to modify the startup configuration file.

Verification

- Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

Related Commands

Modifying the Path for Saving Startup Configurations and the Corresponding File Name

Command	**boot config { flash:***filename* | **usb0:***filename* **}**
Parameter Description	**flash:** Saves the startup configuration file in the extensible Flash. **usb0:** Saves the startup configuration file in USB0 device. The device must have a USB interface into which a USB flash drive is inserted.
Command Mode	Global configuration mode
Usage Guide	Use this command to modify the path for saving startup configurations and the corresponding file name.

Configuration Example

Changing the Path of the Startup Configuration into flash:/Hostname.text

Configuration Steps	• Change the startup configuration file path into flash:/Hostname.text
	Hostname# configure terminal //Enter global configuration mode. Hostname(config)# boot config flash:/Hostname.text//Change the path and file name into flash:/Hostname.text
Verification	• Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

2.4.6 Configuring the Zero Configuration Function

Configuration Effect

- Enable or disable the zero configuration function.

Notes

- The zero configuration function is applicable to the ACS solution only.
- With the zero configuration function, DHCP Snooping Trust is enabled only on the last two electrical ports and all SFP ports of the device by default, regardless of whether the device supports the MGMT port.
- Enabling and disabling the zero configuration function will delete the startup configuration file of the device and trigger device restart.

Configuration Steps

Enabling or Disabling the Zero Configuration Function

- (Optional) Perform this configuration when you need to enable or disable the zero configuration function.

Verification

- Run the **show zcm mod** command to check whether the zero configuration function is enabled.

Related Commands

Enabling or Disabling the Zero Configuration Function

Command	**zcm { enable | disable }**
Parameter Description	**enable:** Enables the zero configuration function. **disable:** Disables the zero configuration function.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable and disable the zero configuration function.

Configuration Example

Enabling the Zero Configuration Function

Configuration Steps	- Enable the zero configuration function.

	`Hostname# zcm enable //Enable the zero configuration function.`
	`%% Warning: After switching mode the device will automatically restart!`
	`% Do you want to switch to zero configuration mode? [yes/no]:y`
	`*Sep 29 12:36:20: %ZCM-5-MODE_SWITCH: The device is reloading due to zero or non-zero configuration mode switch.`

Verification	- Run the **show zcm mode** command to display whether the zero configuration function is enabled.

2.4.7 Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Steps

Configuring Direct Restart

Run the **reload** command in privileged EXEC mode to restart the system immediately.

Configuring Timed Restart

```
reload at hh:mm:ss month day year
```

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The **month day year** parameter is optional. If it is not specified, the system clock time is used by default.

The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

The restart time must be later than the current system time. After you configure a restart plan, do not change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Commands

Restarting a Device

Command	**reload** [**at** { *hh* [:*mm* [:*ss*]] } [*month* [*day* [*year*]]]]
Parameter Description	**at** *hh:mm:ss*: Indicates the time when the system will restart. *month*: Indicates a month of the year, ranging from 1 to 12. *day*: Indicates a date, ranging from 1 to 31. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

2.4.8 Running Batch File Commands

Configuration Effect

Run the commands in batches.

Configuration Steps

Running the execute Command

Run the **execute** command, with the path set to the batch file to be executed.

You can specify the name and content of the batch file on your PC and transfer the file to the device flash memory through TFTP. The batch processing content simulates user input. Therefore, you need to edit the batch file content according to the CLI command configuration sequence. In addition, you need to write the responses to interactive commands to the batch file to ensure normal command execution.

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

Related Commands

Command	**execute** { [**flash:**] *filename* }
Parameter Description	*filename*: Indicates the path for the batch file to be executed.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to run the commands related to a function in batches.

2.5 Monitoring

Displaying

Description	Command
show boot config	Displays the save path and file name.
show clock	Displays the current system time.
show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }	Displays line configurations.
show reload	Displays system restart settings.
show running-config [**interface** *interface*]	Displays the current running configurations of the device or the configurations on an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show this	Displays the current system configurations.
show version [**devices | module | slots**]	Displays system information.
show sessions	Displays the information of each established Telnet client instance.

3 Configuring Lines

3.1 Overview

There are various types of terminal lines on network devices. You can manage terminal lines in groups based on their types. Configurations on these terminal lines are called line configurations. On network devices, terminal lines are classified into multiple types such as CTY, and VTY.

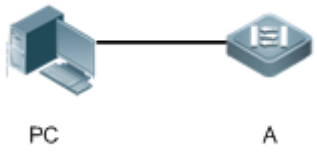
3.2 Applications

Application	Description
Accessing a Device Through Console	Enter the command-line interface (CLI) of a network device through the Console.
Accessing a Device Through VTY	Enter the CLI of a network device through Telnet or SSH.

3.2.1 Accessing a Device Through Console

Scenario

Figure 3-1



Remarks	A is a network device to be managed. PC is a network management station.

Deployment

The network management station connects to the Console port of a network device through a serial cable. Using the Console software (Hyper Terminal or other terminal simulation software) on the network management station, you can access the Console of the network device and enter the CLI to configure and manage the network device.

3.2.2 Accessing a Device Through VTY

Scenario

Figure 3-2



Remarks	A is a network device to be managed. PC is a network management station.

Deployment

The network management station connects to a network device through the network. Using a VTY client (such as Putty) on the network management station, you can access the network device through Telnet or SSH and enter the CLI to configure and manage the network device.

3.3 Features

Basic Concepts

CTY

The CTY line refers to the line connected to the Console port. Most network devices have a Console port. You can access the local system through the Console port.

VTY

The VTY line is a virtual terminal line that does not correspond to any hardware. It is used for Telnet or SSH connection.

Overview

Feature	Description
Basic Features	Configures a terminal, displays and clears terminal connection information.

3.3.1 Basic Features

Related Configuration

Configuring Terminal Lines

Run the **line** command in global configuration mode to enter the configuration mode of a specified line.

Configure the line attributes.

Clearing Terminal Connections

When a terminal connects to the network device, the corresponding terminal line is occupied. Run the **show user** command to display the connection status of these terminal lines. If you want to disconnect the terminal from the network device, run the **clear line** command to clear the terminal line. After the terminal lines are cleared, the related connections (such as Telnet

and SSH) are interrupted, the CLI exits, and the terminal lines restore to the unoccupied status. Users can re-establish connections.

Specifying the Number of VTY Terminals

Run the **line vty** command to enter the VTY line configuration mode and specify the number of VTY terminals.

By default, there are 5 VTY terminals, numbered from 0 to 4. You can increase the number of VTY terminals to 36, with new ones numbered from 5 to 35. Only new terminals can be removed.

3.4 Configuration

Configuration	Description and Command	
Entering Line Configuration Mode	(Mandatory) It is used to enter the line configuration mode.	
	line [**console** | **vty**] *first-line* [*last-line*]	Enters the specified line configuration mode.
	line vty *line-number*	Increases or reduces the number of available VTY lines.

3.4.1 Entering Line Configuration Mode

Configuration Effect

Enter line configuration mode to configure other functions.

Configuration Steps

Entering Line Configuration Mode

- Mandatory.
- Unless otherwise specified, enter line configuration mode on each device to configure line attributes.

Increasing/Reducing the Number of VTY Lines

- Optional.
- Run the (**no**) **line vty** *line-number* command to increase or reduce the number of VTY lines.

Verification

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

Related Commands

Entering Line Configuration Mode

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

Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *first-line*: Indicates the number of the first line. *last-line*: Indicates the number of the last line.
Command Mode	Global configuration mode
Usage Guide	N/A

Increasing/Reducing the Number of VTY Lines

Command	**line vty** *line-number*
Parameter Description	*line-number*: Indicates the number of VTY lines. The value ranges from 0 to 35.
Command Mode	Global configuration mode
Usage Guide	Run the **no line vty** *line-number* command to reduce the number of available VTY lines.

Displaying Line Configuration

Command	**show line** {**console** *line-num*	**vty** *line-num*	*line-num* }
Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *line-num*: Indicates the line to be displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Scenario **Figure 3-3**	
Configuration Steps	● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Run the **show user** command to display the connection status of the terminal line. ● Run the **show line console** 0 command to display the status of the Console line. ● Enter global configuration mode and run the **line vty** command to increase the number of VTY terminals to 36.
A	`Hostname#show user`

```
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- ------------------
*  0 con 0       ---          idle                 00:00:00   ---


Hostname#show line console 0


CON     Type    speed   Overruns
* 0     CON     9600    0
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     ^D          ^M
Timeouts:      Idle EXEC    Idle Session
               00:10:00     never
History is enabled, history size is 10.
Total input: 490 bytes
Total output:  59366 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times


Hostname#show line vty ?
  <0-5>    Line number


Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#line vty 35
Hostname(config-line)#
*Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console
```

Verification

- After running the **show line** command, you can find that the number of terminals increases.
- Run the **show running-config** command to display the configuration.

A

```
Hostname#show line vty ?
```

```
  <0-35>  Line number


Hostname#show running-config


Building configuration...
Current configuration : 761 bytes


version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
 ip address 192.168.23.164 255.255.255.0
!
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
!
line con 0
line vty 0 35
```

	login ! end

3.4.2 Configuring Line Attributes

Configuration Effect

Configure line attributes in line configuration mode.

Configuration Steps

Configuring the Absolute Timeout for Line Disconnection

- Optional.
- Run the **absolute-timeout** command to ensure that a line is disconnected after the specified time.

Configuring the Character You Enter at a Vacant Terminal to Begin a Terminal Session

- Optional.
- Run the **activation-character** command in line configuration mode to configure a character to activate a terminal.

Enabling Automatic Command Execution

- Optional.
- Run the **autocommand** command in line configuration mode to enable automatic command execution on terminals with asynchronous ports.

Configuring the Number of Data Bits per Character for Physical Terminal Connections

- Optional.
- Run the **databits** command in line configuration mode.

Configuring the EXEC Character Width for Physical Terminal Connections

- Optional.
- Run the **exec-character-bits** command in line configuration mode.

Configuring Flow Control Mode for Physical Terminal Connections

- Optional.
- Run the **flowcontrol** command in line configuration mode.

Configuring the Parity Bit for Physical Terminal Connections

- Optional.
- Run the **parity** command in line configuration mode.

Configuring the Start Character of Software Flow Control for Physical Terminal Connections

- Optional.
- Run the **start-character** command in line configuration mode.

Configuring the Stop Character of Software Flow Control for Physical Terminal Connections

- Optional.
- Run the **stop-character** command in line configuration mode.

Configuring the Number of Stop Bits per Byte for Physical Terminal Connections

- Optional.
- Run the **stopbits** command in line configuration mode.

Configuring the Type of Terminal Connected to a Line

- Optional.
- Run the **terminal-type** command in line configuration mode.

Verification

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

Related Commands

Configuring the Absolute Timeout for Line Disconnection

Command	**absolute-timeout** *minutes*
Parameter Description	*minutes*: Indicates the absolute timeout of the current line in minutes. The value ranges from 0 to 60.
Command Mode	Line configuration mode
Usage Guide	Configure the absolute timeout for line disconnection. As long as the specified time expires, the line is disconnected no matter whether you are on the operating terminal or not. Before the line is disconnected, the system displays the remaining time after which the terminal will exit: `Terminal will be login out after 20 second`

Configuring the Character You Enter at a Vacant Terminal to Begin a Terminal Session

Command	**activation-character** *ascii-value*
Parameter Description	*ascii-value*: Indicates the ASCII value of the hotkey character for beginning a terminal session. The value ranges from 0 to 127.
Command Mode	Line configuration mode
Usage Guide	If auto-selection is enabled for the current line, the hotkey character for beginning a terminal session must

	be set to the default value.

Enabling Automatic Command Execution

Command	**autocommand** *autocommand-string*
Parameter Description	*autocommand-string*: Indicates the command line to be automatically executed.
Command Mode	Line configuration mode
Usage Guide	In most cases, after a user acts as a dumb terminal to connect to a device through an asynchronous serial port, the user can remotely log in to the specified host through Telnet or obtain the specified application-based terminal service with the **autocommand** command.

Configuring the Number of Data Bits per Character for Physical Terminal Connections

Command	**databits** *bit*
Parameter Description	*bit*: Indicates the number of data bits per character. The value ranges from 5 to 8.
Command Mode	Line configuration mode
Usage Guide	The asynchronous hardware (such as an asynchronous serial port and AUX port) of a device generates seven data bits with parity in flow communication mode. If parity is being generated, specify 7 data bits per character. If no parity is being generated, specify 8 data bits per character. Only early devices support 5 or 6 data bits, which are seldom used.

Configuring the EXEC Character Width for Physical Terminal Connections

Command	**exec-character-bits { 7 | 8 }**
Parameter Description	**7**: Selects the 7-bit ASCII character set. **8**: Selects the 8-bit ASCII character set.
Command Mode	Line configuration mode
Usage Guide	If you need to enter Chinese characters or display Chinese characters, images, or other international characters in the command line, run the **exec-character-bits 8** command.

Configuring Flow Control Mode for Physical Terminal Connections

Command	**flowcontrol { hardware | none | software }**
Parameter Description	**hardware**: Configures hardware flow control. **none**: Configures no flow control. **software**: Configures software flow control.
Command Mode	Line configuration mode
Usage Guide	By running this 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 serves to prevent data loss. When high-data-rate devices communicate with low-rate-data devices (e.g., a printer communicates with a network port), you also need to enable flow control to prevent data loss. The general operating system provides two flow control modes: software flow control (controlled with control keys) and hardware flow control (controlled by hardware). The default stop character and start character for software flow control are respectively Ctrl+S (XOFF, with the ASCII value 19) and Ctrl+Q (XON, with the ASCII value 17). You can also run the **stop-character** and **start-character** commands to configure them.

Configuring the Parity Bit for Physical Terminal Connections

Command	**parity { even | none | odd }**
Parameter Description	**even**: Indicates the even parity check. **none**: Indicates no parity check. **odd**: Indicates the odd parity check.
Command Mode	Line configuration mode
Usage Guide	When using certain hardware (such as an asynchronous serial port and Console port) for communication, you are usually required to configure a parity bit.

Configuring the Start Character of Software Flow Control for Physical Terminal Connections

Command	**start-character** *ascii-value*
Parameter Description	*ascii-value*: Indicates the ASCII value of the start character of software flow control for physical terminal connections. The value ranges from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	After software flow control is enabled, the start character for software flow control indicates the start of data transmission.

Configuring the Stop Character of Software Flow Control for Physical Terminal Connections

Command	**stop-character** *ascii-value*
Parameter Description	*ascii-value*: Indicates the ASCII value of the stop character of software flow control for physical terminal connections. The value ranges from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	After software flow control is enabled, the stop character for software flow control indicates the end of data transmission.

Configuring the Number of Stop Bits per Byte for Physical Terminal Connections

Command	**stopbits { 1 | 2 }**
Parameter Description	**1**: Indicates one stop bit. **2**: Indicates two stop bits.
Command	Line configuration mode

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

Configuring the Type of Terminal Connected to a Line

Command	**terminal-type** *terminal-type-string*
Parameter Description	*terminal-type-string*: Indicates the description of the terminal type, such as vt100 and ansi.
Command Mode	Line configuration mode
Usage Guide	You can run the **terminal-type vt100** command to restore the default terminal type or run the **terminal-type** command to configure the type of 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 ID: 0x18). For details, see RFC 854.

Configuration Example

Configuring the Baud Rate, Data Bits, Parity Bits, and Stop Bits

Scenario Figure 3-4	
Configuration Steps	● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Configure the baud rate, data bits, parity bit, and stop bits in global configuration mode. ● Run the **show line console** 0 command to display the status of the Console line.

A	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#line console 0`
	`Hostname(config-line)#speed 115200`
	`Hostname(config-line)#databits 8`
	`Hostname(config-line)#parity even`
	`Hostname(config-line)#stopbits 1`
	`Hostname#show line console 0`
	
	`CON     Type    speed   Overruns`
	`* 0     CON     115200  0`

```
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     none
Timeouts:      Idle EXEC    Idle Session
               00:10:00     never
History is enabled, history size is 10.
Total input: 636 bytes
Total output:  30498 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
```

Verification

- Run the **show running-config** command to display the configuration.

A

```
Hostname#show line vty ?
  <0-35>  Line number

Hostname#show running-config

Building configuration...
Current configuration : 761 bytes

version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
 ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
```

```
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
line con 0
 parity even
 stopbits 1
 speed 115200
line vty 0 35
 login
!
end
```

3.4.3 Configuring Terminal Attributes

Configuration Effect

Configure terminal attributes in privileged EXEC mode of a terminal.

Configuration Steps

↘ **Configuring the Number of Data Bits per Character for the Current Session**

- Optional.
- Run the **terminal databits** command on the terminal.

↘ **Configuring the EXEC Character Width for the Current Session**

- Optional.
- Run the **terminal exec-character-bits** command on the terminal.

↘ **Configuring Flow Control Mode for the Current Session**

- Optional.
- Run the **terminal flowcontrol** command on the terminal.

Configuring the Parity Bits for the Current Session

- Optional.
- Run the **terminal parity** command on the terminal.

Configuring the Start Character of Software Flow Control for the Current Session

- Optional.
- Run the **terminal start-character** command on the terminal.

Configuring the Stop Character of Software Flow Control for the Current Session

- Optional.
- Run the **terminal stop-character** command on the terminal.

Configuring the Number of Stop Bits in Each Byte for the Current Session

- Optional.
- Run the **terminal stopbits** command on the terminal.

Configuring the Type of Terminal Connected to the Current Line for the Current Session

- Optional.
- Run the **terminal terminal-type** command on the terminal.

Verification

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

Related Commands

Configuring the Number of Data Bits per Character for the Current Session

Command	**terminal databits** *bit*
Parameter Description	*bit*: Indicates the number of data bits per character, ranging from 5 to 8.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the EXEC Character Width for the Current Session

Command	**terminal exec-character-bits { 7 | 8 }**
Parameter Description	**7**: Selects the 7-bit ASCII character set. **8**: Selects the full 8-bit ASCII character set.
Command	Privileged EXEC mode

Mode	
Usage Guide	If you need to enter Chinese characters or display Chinese characters, images, or other international characters in the command line, run the **terminal exec-character-bits 8** command.

Configuring Flow Control Mode for the Current Session

Command	**terminal flowcontrol { hardware | none | software }**
Parameter Description	**hardware**: Configures hardware flow control. **none**: Configures no flow control. **software**: Configures software flow control.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Parity Bit of the Asynchronous Line for the Current Session

Command	**terminal parity { even | none | odd }**
Parameter Description	**even**: Indicates the even parity check. **none**: Indicates no parity check. **odd**: Indicates the odd parity check.
Command Mode	Line configuration mode
Usage Guide	When using certain hardware (such as an asynchronous serial port and Console port) for communication, you are usually required to configure a parity bit.

Configuring the Start Character of Software Flow Control for the Current Session

Command	**terminal start-character** *ascii-value*
Parameter Description	*ascii-value*: Indicates the ASCII value of the start character of software flow control for the current session. The value ranges from 0 to 255.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Stop Character of Software Flow Control for the Current Session

Command	**terminal stop-character** *ascii-value*
Parameter Description	*ascii-value*: Indicates the ASCII value of the stop character of for the current session. The value ranges from 0 to 255.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Number of Stop Bits for the Current Session

Command	**terminal stopbits { 1 | 2 }**
Parameter Description	**1**: Indicates one stop bit. **2**: Indicates two stop bits.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Type of Terminal Connected to the Current Line for the Current Session

Command	**terminal terminal-type** *terminal-type-string*
Parameter Description	*terminal-type-string*: Indicates the description of the terminal type, such as vt100 and ansi.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Configuring the Terminal Type and Baud Rate of a Terminal

Scenario Figure 3-5	
Configuration Steps	● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Configure the terminal type and baud rate of the terminal in privileged EXEC mode.
A	`Hostname#terminal terminal-type ansi` `Hostname#terminal speed 115200`
Verification	● Run the **show line console** 0 command to display the status of the Console line.

A	`Hostname#show line console 0`
	
	`CON Type speed Overruns`
	`* 0 CON 115200 0`
	`Line 0, Location: "", Type: "ansi"`
	`Length: 24 lines, Width: 79 columns`
	`Special Chars: Escape Disconnect Activation`
	`^^x none`
	`Timeouts: Idle EXEC Idle Session`

```
                00:10:00     never

History is enabled, history size is 10.

Total input: 858 bytes

Total output:  57371 bytes

Data overflow:  0 bytes

stop rx interrupt:  0 times
```

3.5 Monitoring

Clearing

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

Description	Command
Clears the line connection status.	**clear line** { **console** *line-num* | **vty** *line-num* | *line-num* }

Displaying

Description	Command
Displays the line configuration.	**show line** { **console** *line-num* | **vty** *line-num* | *line-num* }
Displays historical records of a line.	**show history**
Displays the privilege level of a line.	**show privilege**
Displays users on a line.	**show user** [**all**]

4 Configuring Time Range

4.1 Overview

Time Range is a time-based control service that provides some applications with time control. For example, you can configure a time range and associate it with an access control list (ACL) so that the ACL takes effect within certain time periods of a week.

4.2 Typical Application

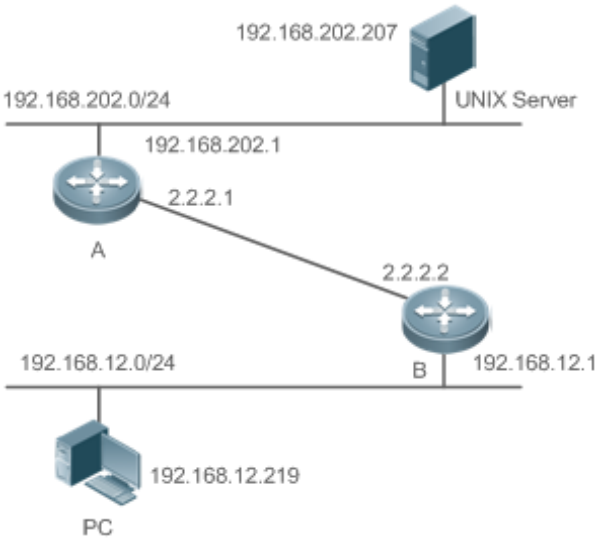
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

4.2.1 Applying Time Range to an ACL

Application Scenario

An organization allows users to access the Telnet service on a remote Unix host during working hours only, as shown in Figure 4-1.

Figure 4-1



Note	Configure an ACL on device B to implement the following security function: Hosts in network segment 192.168.12.0/24 can access the Telnet service on a remote Unix host during normal working hours only.

Functional Deployment

- On device B, apply an ACL to control Telnet service access of users in network segment 192.168.12.0/24. Associate the ACL with a time range, so that the users' access to the Unix host is allowed only during working hours.

4.3 Function Details

Basic Concepts

Absolute Time Range

The absolute time range is a time period between a start time and an end time. For example, [12:00 January 1 2000, 12:00 January 1 2001] is a typical absolute time range. When an application based on a time range is associated with the time range, a certain function can be effective within this time range.

Periodic Time

Periodic time refers to a periodical interval in the time range. For example, "from 8:00 every Monday to 17:00 every Friday" is a typical periodic time interval. When a time-based application is associated with the time range, a certain function can be effective periodically from every Monday to Friday.

Features

Feature	Function
Using Absolute Time Range	Sets an absolute time range for a time-based application, so that a certain function takes effect within the absolute time range.
Using Periodic Time	Sets periodic time or a time-based application, so that a certain function takes effect within the periodic time.

4.3.1 Using Absolute Time Range

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the absolute time range. If yes, the function is effective or ineffective at the current time depending on specific configuration.

4.3.2 Using Periodic Time

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the period time. If yes, the function is effective or ineffective at the current time depending on specific configuration.

4.4 Configuration Details

Configuration Item	Suggestions and Related Commands	
Configuring Time Range	⚠ Mandatory configuration. Time range configuration is required so as to use the time range function.	
	time-range *time-range-name*	Configures a time range.
	⚠ Optional configuration. You can configure various parameters as necessary.	
	absolute { [**start** *time date*] | [**end** *time date*] }	Configures an absolute time range.
	periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*	Configures periodic time.

4.4.1 Configuring Time Range

Configuration Effect

- Configure a time range, which may be an absolute time range or a periodic time interval, so that a time-range-based application can enable a certain function within the time range.

Configuration Method

↘ **Configuring Time Range**

- Mandatory configuration.
- Perform the configuration on a device to which a time range applies.

↘ **Configuring Absolute Time Range**

- Optional configuration.

↘ **Configuring Periodic Time**

- Optional configuration.

Verification

- Use the **show time-range** [*time-range-name*] command to check time range configuration information.

Related Commands

↘ **Configuring Time Range**

Command Syntax	**time-range** *time-range-name*
Parameter Description	*time-range-name*: name of the time range to be created.

Command Mode	Global configuration mode
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range, then you can configure relevant time control in time range configuration mode.

Configuring Absolute Time Range

Command Syntax	**absolute** { [**start** *time date*] | [**end** *time date*] }
Parameter Description	**start** *time date*: start time of the range. **end** *time date*: end time of the range.
Command Mode	Time range configuration mode
Usage Guide	Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

Configuring Periodic Time

Command Syntax	**periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*
Parameter Description	*day-of-the-week*: the week day when the periodic time starts or ends *time*: the exact time when the periodic time starts or ends
Command Mode	Time range configuration mode
Usage Guide	Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

4.5 Monitoring and Maintaining Time Range

Displaying the Running Status

Function	Command
Displays time range configuration.	**show time-range** [*time-range-name*]

5 Configuring HTTP Service

5.1 Overview

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 connection-oriented Transmission Control Protocol (TCP).

Hypertext Transfer Protocol Secure (HTTPS) is an HTTP supporting the Secure Sockets Layer (SSL) protocol. HTTPS is mainly used to create a secure channel on an insecure network, ensure that information can hardly be intercepted, and provide certain reasonable protection against main-in-the-middle attacks. At present, HTTPS is widely used for secure and sensitive communication on the Internet, for example, electronic transactions.

Protocols and Standards

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

5.2 Applications

Application	Description
HTTP Application Service	Users manage devices based on Web.

5.2.1 HTTP Application Service

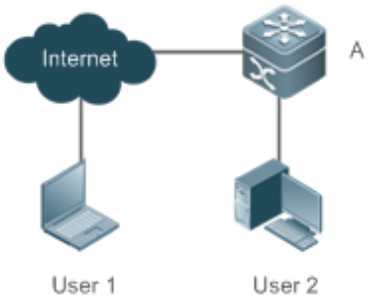
Scenario

After the HTTP service is enabled, users can access the Web management page after passing authentication by only entering **http://IP address of a device** in the browser of a PC. On the Web page, users you can monitor the device status, configure devices, upload and download files.

Take the following figure as an example to describe Web management.

- Users can remotely access devices on the Internet or configure and manage devices on the Local Area Network (LAN) by logging in to the Web server.
- According to actual conditions, users can choose to enable the HTTPS or HTTP service or enable the HTTPS and HTTP services at the same time.
- Users can also access the HTTP service of devices by setting and using HTTP/1.0 or HTTP/1.1 in the browser.

Figure 5-1



Remarks	A is a device. User 1 accesses the device through the Internet. User 2 accesses the device through a LAN.

Deployment

- When a device runs HTTP, users can access the device by entering **http://IP address of the device** in the browser of a PC.
- When a device runs HTTPS, users can access the device by entering **https://IP address of the device** in the browser of a PC.

5.3 Features

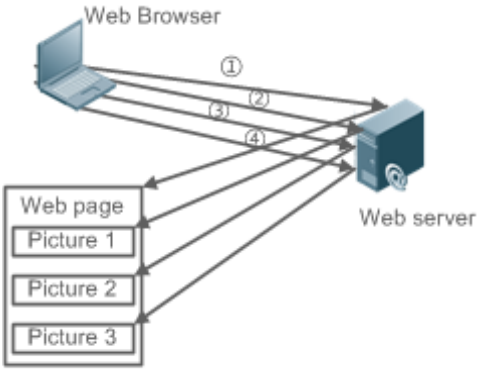
Basic Concepts

HTTP Service

The HTTP service refers to transmission of Web page information on the Internet by using HTTP. HTTP/1.0 is currently an HTTP version that is the most widely used. As one Web server may receive thousands or even millions of access requests, HTTP/1.0 adopts the short connection mode to facilitate connection management. One TCP connection is established for each request. After a request is completed, the TCP connection is released. The server does not need to record or trace previous requests. Although HTTP/1.0 simplifies connection management, HTTP/1.0 introduces performance defects.

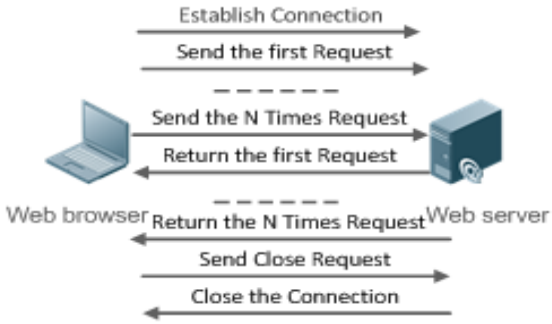
For example, a web page my need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is completely isolated. Establishing and releasing connections is a relatively troublesome process, which severely affects the performance of the client and server, as shown in the following figure:

Figure 5-2



HTTP/1.1 overcomes the defect. It supports persistent connection, that is, one connection can be used to transmit multiple requests and response messages. In this way, a client can send a second request without waiting for completion of the previous request. This reduces network delay and improves performance. See the following figure:

Figure 5-3



At present, the devices support both HTTP/1.0 and HTTP/1.1.

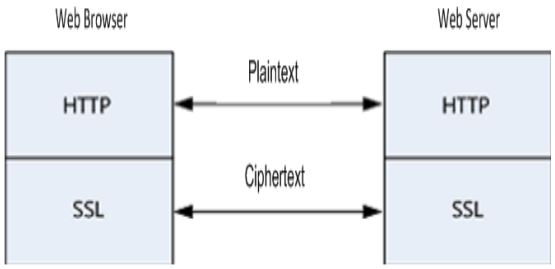
Which HTTP version will be used by a device is decided by the Web browser.

HTTPS Service

The HTTPS service adds the SSL based on the HTTP service. Its security basis is the SSL. To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not necessarily need one. The SSL protocol provides the following services:

- Authenticating users and servers and ensuring that data is sent to the correct client and server.
- Encrypting data to prevent data from being stolen midway.
- Maintaining data integrity and ensuring that data is not changed during transmission.

Figure 5-4



- During a local upgrade, a device serves as an HTTP server. Users can log in to the device through a Web browser and upload upgrade files to the device to realize file upgrade on the device.

Features

Feature	Description
HTTP Service	Users log in to devices through Web pages to configure and manage devices.
Local HTTP Upgrade Service	Upgrade files are uploaded to a device to realize file upgrade on the device.

5.3.1 HTTP Service

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

Working Principle

Web management covers Web clients and Web servers. Similarly, the HTTP service also adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It can send HTTP packets and receive HTTP response packets. The Web server (namely 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 ID of the HTTP service is 80 and the default port ID of the HTTPS service is 443.
- The client sends a request message to the server.
- The server resolves the request message sent by the client. The request content includes obtaining a Web page, executing a CLI command, and uploading a file.
- After executing the request content, the server sends a response message to the client.

Related Configuration

↘ **Enabling the HTTP Service**

By default, the HTTP service is disabled.

The **enable service web-server** command can be used to enable HTTP service functions, including the HTTP service and HTTPS service.

The HTTP service must be enabled so that users can log in to devices through Web pages to configure and manage devices.

↘ Configuring HTTP Authentication Information

By default, the system creates the **admin** account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the admin account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.

The **webmaster level** command can be used to configure an authenticated user name and a password.

After this command is run, you need to enter the configured user name and password to log in to the Web page.

↘ Configuring an HTTP Service Port

By default, the HTTP service port ID is 80.

The **http port** command can be used to configure an HTTP service port ID. The value range of the port ID is 80 and 1025 to 65535.

By configuring an HTTP service port ID, you can reduce the number of attacks initiated by illegal users on the HTTP service.

↘ Configuring an HTTPS Service Port

By default, the HTTPS service port ID is 443.

The **http secure-port** command can be used to configure an HTTPS service port ID. The value range of the port ID is 443 and 1025 to 65535.

By configuring an HTTPS service port ID, you can reduce the number of attacks initiated by illegal users on the HTTPS service.

5.3.2 Local HTTP Upgrade Service

When a device serves as the HTTP server, users can log in to the device through a Web browser and upload upgrade files (including component package and Web package) to the device or directly upload files to the device through Trivial File Transfer Protocol (TFTP).

Working Principle

- A component package or Web package is uploaded through the local upgrade function provided by Web.
- After successfully receiving a file, the device checks the version for its validity.
- After the file check is successful, if the file is a Web package, perform the upgrade directly; if the file is a component package, decide whether to perform the upgrade in the browser by restarting the device.

Related Configuration

Updating a Web Package

Run the **upgrade web download** command to download a Web package from the TFTP server.

After the command is run, download a Web package from the TFTP server. After the package passes the validity check, directly use the Web package for upgrade without restarting the device.

You can also run the **upgrade web** command to directly upgrade a Web package stored locally.

Updating a Subsystem Component

By default, a device does not upgrade subsystem components uploaded through a browser or TFTP.
To upgrade a subsystem component, you must restart the device.

5.4 Configuration

Configuration	Description and Command	
Configuring the HTTP Service	(Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	webmaster level	Configures HTTP authentication information.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring HTTP redirection to HTTPS	(Optional) It is used to configure HTTP redirection to HTTPS.	
	web-server http redirect-to-https	Configures HTTP redirection to HTTPS.
Configuring HTTPS Certificate	(Optional) It is used to configure HTTPS certificate.	
	web-server https generate self-signed-certificate	Re-generates HTTP self-signed certificate.
	web-server https certificate	Installs HTTPS certificate.
Configuring a Local HTTP Upgrade	(Mandatory) It is used to realize a local HTTP upgrade.	
	upgrade web	Upgrades a Web package stored on a device.
	upgrade web download	Automatically downloads a Web package from a server and automatically upgrades the package.

5.4.1 Configuring the HTTP Service

Configuration Effect

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

Configuration Steps

Enabling the HTTP Service

- Mandatory
- If there is no special requirement, enable the HTTP service on devices. Otherwise, the Web service is inaccessible.

Configuring HTTP Authentication Information

- By default, the user name **admin** and the password **admin** are configured.
- If there is no special requirement, you can log in to the Web page by using the default user name and directly update authentication information through the Web browser. If you always use the default account, security risks may exist because unauthorized personnel can obtain device configuration information once the IP address is disclosed.

Configuring an HTTP Service Port

- If an HTTP service port needs to be changed, the HTTP service port must be configured.
- If there is no special requirement, the default HTTP service port 80 can be used for access.

Configuring an HTTPS Service Port

- If an HTTPS service port needs to be changed, the HTTPS service port must be configured.
- If there is no special requirement, the default HTTPS service port 443 can be used for access.

Verification

- Enter **http://IP address of the device: service port** to check whether the browser skips to the authentication page.
- Enter **https://IP address of the device: service port** to check whether the browser skips to the authentication page.

Related Commands

Enabling the HTTP Service

Command	**enable service web-server** [**http** | **https** | **all**]
Parameter Description	**http** | **https** | **all**: Enables the corresponding service. **http** indicates enabling the HTTP service, **https** indicates enabling the HTTPS service, and **all** indicates enabling the HTTP and HTTPS services at the same time. By default, the HTTP and HTTPS services are enabled at the same time.
Command Mode	Global configuration mode.
Usage Guide	If no key word or **all** is put at the end of the command when the command is run, the HTTP and HTTPS services are enabled at the same time. If the key word **http** is put at the end of the command, only the HTTP service is enabled; if the key word **https** is put at the end of the command, only the HTTPS service is enabled.

	The **no enable service web-server** or **default enable service web-server** command is used to disable the corresponding HTTP service. If no key word is put at the end of the **no enable service web-server** or **default enable service web-server** command, the HTTP and HTTPS services are disabled.

Configuring HTTP Authentication Information.

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }
Parameter Description	*privilege-level*: Permission level bound to a user. *name*: User name. *password*: User password. **0 | 7**: Password encryption type. 0: no encryption; 7: simple encryption. The default value is **0**. *encrypted-password*: Password text.
Command Mode	Global configuration mode.
Usage Guide	When the HTTP server is used, you need to be authenticated before logging in to the Web page. The **webmaster level** command is used to configure a user name and a password for logging in to the Web page. Run the **no webmaster level** *privilege-level* command to delete all user names and passwords of the specified permission level. Run the **no webmaster level** *privilege-level* **username** *name* command to delete the specified user name and password. User names and passwords involve three permission levels: Up to 10 user names and passwords can be configured for each permission level. By default, the system creates the **admin** account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the **admin** account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.

Configuring an HTTP Service Port

Command	**http port** *port-number*
Parameter Description	*port-number*: Configures an HTTP service port. The value range is 80 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTP service port.

Configuring an HTTPS Service Port

Command	**http secure-port** *port-number*
Parameter	*port-number*: Configures an HTTPS service port. The value range is 443 and 1025 to 65535.

Description	
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTPS service port.

Configuration Example

Managing one Device by Using Web and Logging in to the Web Management System through a Web Browser to Configure Related Functions

- Log in to the device by using the **admin** account configured by default.
- To improve security, the Web browser is required to support both HTTP and HTTPS for access.
- You are required to configure an HTTP service port to reduce the number of attacks initiated by illegal users on HTTP.

Scenario Figure 5-5	
Configuration Steps	• Enable the HTTP and HTTPS services at the same time. • Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.
A	A#configure terminal A(config)# enable service web-server A(config)# http port 8080 A(config)# http secure-port 4430
Verification	Check HTTP configurations.
A	A# show web-server status http server status: enabled http server port: 8080 https server status:enabled https server port: 4430

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 devices on the Web client.

5.4.2 Configuring HTTP Redirection to HTTPS

Configuration Effect

After enabling HTTP and HTTPS, users can configure HTTP redirection to HTTPS to improve security.

Configuration Steps

HTTP Redirection to HTTPS

- HTTP redirection to HTTPS is disabled by default.
- Run the **web-server http redirect-to-https** command to enable HTTP redirection to HTTPS.
- Configure HTTP redirection to HTTPS to improve security.

Command	**web-server http redirect-to-https**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no web-server http redirect-to-https** or **default web-server http redirect-to-https** command to configure HTTP redirection to HTTPS.

HTTP and HTTPS must be enabled first.

If the target IP address is a NAPT address, HTTP redirection to HTTPS may fail. In this case, please disable HTTP first and use HTTPS to access this IP address.

Verification

- Enter **http://Device IP:HTTP port** into the address bar of the browser to verify whether the browser will redirect to **http://Device IP:HTTP port**.
- Run the **show web-server status** command to configure HTTP redirection to HTTPS.

Configuration Example

Using Browser to Access Web

- Configure HTTP redirection to HTTPS to improve security.

Scenario

Figure 5-6



Configuration Steps

- Enable both HTTP and HTTPS.
- Configure HTTP redirection to HTTPS.

A

```
A#configure terminal
A(config)# enable service web-server
```

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

Verification

- Check Web status.
- Enter **http://Device IP:HTTP port** into the address bar of the browser to verify whether the browser will redirect to **http://Device IP:HTTP port**.

A

```
A(config)#show web-server status
http server status: enabled
http server port: 80
https server status:enabled
https server port: 443
http redirect to https: true
```

5.4.3 Configuring HTTPS Certificate

Configuration Effect

Configure HTTPS certificate to re-generate the self-signed certificate or the certificate assigned by Certificate Authority.

Configuration Steps

Re-generating HTTPS Self-signed Certificate

- HTTPS self-signed certificate is used by default.
- Run the **web-server https generate self-signed-certificate** command to re-generate the HTTPS certificate.

Command	**web-server https generate self-signed-certificate**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is an interactive command. After running this command, please enter the information required or press Ctrl+C to abort the task. If the HTTPS certificate is installed, the HTTPS certificate will be used preferentially. The re-generated self-signed certificate will not replace the HTTPS certificate. This command is not displayed in running-config. It is recommended to open the Web management page again after closing the browser.

Installing HTTPS Certificate

- HTTPS self-signed certificate is used by default.

- Run the **web-server https certificate** command to install the HTTPS certificate.
- Installing the HTTPS certificate assigned by the Certificate Authority will prevent distrust prompt popping up during HTTPS access.

Command	**web-server https certificate** { **pem** *cert-filename* **private-key** *key-filename* } | { **pfx** *cert-filename* } [**password** *password-text*]
Parameter Description	**pem**: Imports the certificate and private key file in pem format. **pfx**: Imports the certificate file in pfx format. *cert-filename*: Specifies the name of the certificate file under the flash: directory. *key-filename*: Specifies the name of the private key file under the flash: directory. **password** *password-text*: Configures the decryption password.
Command Mode	Global configuration mode
Usage Guide	Run the **copy** command to copy the certificate/private key file to the **flash:** partition. After installation finishes, the certificate/private key file can be deleted. You can run the **no web-server https certificate** command to delete the HTTPS certificate. Afterwards, the auto-signed HTTPS certificate will be used. This command is not displayed in running-config. It is recommended to open the Web management page again after closing the browser.

Verification

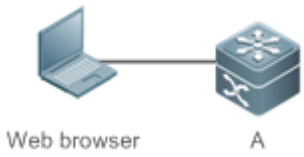
- Run the **show web-server https certificate information** command to display HTTPS certificate.

Configuration Example

Re-generating HTTPS Self-signed Certificate

Scenario

Figure 5-7



Configuration Steps

A

- Re-generate the self-signed certificate.

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

Verification

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

A

```
A#show web-server https certificate information
Source: Default
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Self-Signed-600B16C2
        Validity
            Not Before: Feb 28 05:49:39 2019 GMT
            Not After : Feb 25 05:49:39 2029 GMT
        Subject: CN=Self-Signed-600B16C2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
.....
A#
```

Installing Third-party HTTPS Certificate

- The certificate file name is usercert.pfx and the key is 123456. Enable the TFTP server and place the certificate file under the TFTP server directory.

Scenario

Figure 5-8



Configuration Steps

- Run the **copy** command to copy the certificate/private key file to the **flash:** partition.
- Run the **web-server https certificate** command to install HTTPS certificate.

A

```
A# copy tftp://192.168.1.1/usercert.pfx flash:usercert.pfx
Press Ctrl+C to quit
!
```

```
Copy success.
A#configure terminal
A(config)# web-server https certificate pfx usercert.pfx password 123456
*Feb 28 14:38:37: %HTTPD-4-CERT_CHANGE: HTTPS certificate changed.
% The certificate was successfully installed.
```

Verification A

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

```
A#show web-server https certificate information
Source: Installed
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, CN=mytestCA
        Validity
            Not Before: Jan 23 08:36:21 2019 GMT
            Not After : Jan 23 08:36:21 2020 GMT
        Subject: C=CN, CN=test-cert-2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
.....
 A#
```

5.4.4 Configuring a Local HTTP Upgrade

Configuration Effect

Perform an HTTP upgrade through the browser or the **upgrade web** command.

Notes

- So long as a Web package is uploaded successfully and passes the version check, the device directly performs an upgrade based on the latest Web package.
- The **upgrade web download** command is used to automatically download files from the TFTP server and automatically perform an upgrade.
- The **upgrade web** command is used to automatically upgrade the Web package in the local file system.

Configuration Steps

N/A

Verification

- Access and view the latest Web page through the browser.

Related Commands

Downloading a Web Package from the TFTP Server

Command	**upgrade download tftp:** *path*
Parameter Description	**tftp**: Connects the FTFP server through a common data port and downloads a Web package. *path*: Path of a Web package on the TFTP server.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to download a Web package from the TFTP server and automatically perform an upgrade.

Upgrading a Web Package Stored on a Local Device

Command	**upgrade web** *uri*
Parameter Description	*uri*: Local path for storing a Web package.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to upgrade a Web package stored on a device and automatically perform an upgrade.

Configuration Example

Obtaining the Latest Web Package from the Official Website and Running the Web Package

Scenario Figure 5-9	
Configuration Steps	● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Log in to the device through Web and upload the latest Web package to the device.
A	A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0

	A(config-VLAN 1)# exit A(config)# enable service web-server
	On a PC, use the local upgrade function on the Web page to upload a Web package for upgrade.
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Upgrading a Web Package by Running the upgrade web download Command

Scenario **Figure 5-10**	
Configuration Steps	● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.
A	A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#upgrade web download tftp:// 10.10.10.13/web.upd Press Ctrl+C to quit !!!!!!!! download 3896704 bytes Begin to upgrade the web package... Web package upgrade successfully.
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Upgrading a Web Package by Running the upgrade web Command

Scenario **Figure 5-11**	
Configuration Steps	● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.

A	A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#copy tftp://10.10.10.13/web.upd flash:/web.upd Press Ctrl+C to quit !!!!!!!! Accessing tftp:// 10.10.10.13/web.upd finished, 3896704 bytes prepared Flushing data to flash:/web.upd... Flush data done A #upgrade web flash:/web.upd Web package upgrade successfully. A #
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Common Errors

- Access to the web page through the browser shows that the web page is not updated based on the latest Web package. This is possibly because the local browser has a cache. Clear the cache of the local browser and access the Web page again.

5.5 Monitoring

Displaying

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

6 Configuring Syslog

6.1 Overview

Status changes (such as link up and down) or abnormal events may occur anytime. The products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

Protocols and Standards

- RFC3164: The BSD syslog Protocol
- RFC5424: The_Syslog_Protocol

6.2 Applications

Application	Description
Sending Syslogs to the Console	Monitor syslogs through the Console.
Sending Syslogs to the Log Server	Monitor syslogs through the server.

6.2.1 Sending Syslogs to the Console

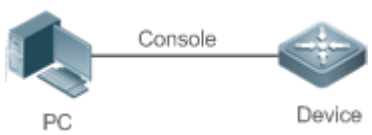
Scenario

Send syslogs to the Console to facilitate the administrator to monitor the performance of the system. The requirements are as follows:

1. Send logs of Level 6 or higher to the Console.
2. Send logs of only the ARP and IP modules to the Console.

Figure 6-1 shows the network topology.

Figure 6-1 Network topology



Deployment

Configure the device as follows:

1. Set the level of logs that can be sent to the Console to informational (Level 6).
2. Set the filtering direction of logs to terminal.
3. Set log filtering mode of logs to contains-only.
4. Set the filtering rule of logs to single-match. The module name contains only ARP or IP.

6.2.2 Sending Syslogs to the Log Server

Scenario

Send syslogs to the log server to facilitate the administrator to monitor the logs of devices on the server. The requirements are as follows:

1. Send syslogs to the log server 10.1.1.1.
2. Send logs of Level 7 or higher to the log server.
3. Send syslogs from the source interface Loopback 0 to the log server.

Figure 6-2 shows the network topology.

Figure 6-2 Network topology



Deployment

Configure the device as follows:

1. Set the IPv4 address of the server to 10.1.1.1.
2. Set the level of logs that can be sent to the log server to debugging (Level 7).
3. Set the source interface of logs sent to the log server to Loopback 0.

6.3 Features

Basic Concepts

Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

Levels of Syslogs

Eight severity levels of syslogs are defined in descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging. These levels correspond to eight numerical values from 0 to 7. A smaller value indicates a higher level.

Only logs with a level equaling to or higher than the specified level can be output. For example, if the level of logs is set to informational (Level 6), logs of Level 6 or higher will be output.

The following table describes the log levels.

Level	Numerical Value	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that the measures must be taken immediately.
critical	2	Indicates a critical condition.
errors	3	Indicates an error.
warnings	4	Indicates a warning.
notifications	5	Indicates a notification message that requires attention.
informational	6	Indicates an informational message.
debugging	7	Indicates a debugging message.

Output Direction of Syslogs

Output directions of syslogs include 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.

The following table describes output directions of syslogs.

Output Direction	Description	Default Output Level	Description
Console	Console	Debugging (Level 7)	Logs and debugging information are output.
monitor	Monitoring terminal	Debugging (Level 7)	Logs and debugging information are output.
server	Log server	Informational (Level 6)	Logs and debugging information are output.
buffer	Log buffer	Debugging (Level 7)	Logs and debugging information are output. The log buffer is used to store syslogs.
file	Log file	Informational (Level 6)	Logs and debugging information are output. Logs in the log buffer are periodically written into files.

RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

- If the output direction is the Console, monitor, buffer, or file, the syslog format is as follows:

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

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

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

- If the output direction is the log server, the syslog format is as follows:

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

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

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

The following describes each field in the log in details:

Priority

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

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

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 syslogs
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
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)

Sequence Number

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

Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Devices support two syslog timestamp formats: datetime and uptime.

If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.

The two timestamp formats are described as follows:

- Datetime format

The datetime format is as follows:

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

The following table describes each parameter of the datetime.

Timestamp Parameter	Parameter Name	Description
Mmm	Month	Mmm refers to abbreviation of the current month. The 12 months in a year are written as Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
dd	Day	dd indicates the current date.
yyyy	Year	yyyy indicates the current year, and is not displayed by default.
hh	Hour	hh indicates the current hour.
mm	Minute	mm indicates the current minute.
ss	Second	ss indicates the current second.
msec	Millisecond	msec indicates the current millisecond.

By default, the datetime timestamp displayed in the syslog does not contain the year and millisecond. You can run a command to display or hide the year and millisecond of the datetime timestamp.

- Uptime format

The uptime format is as follows:

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

The timestamp string indicates the accumulated days, hours, minutes, and seconds since the system is started.

1. Sysname

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

Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which may include upper-case letters, digits, or underscore. The mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

Content

This field indicates the detailed content of the syslog.

RFC5424 Log Format

The syslog format in the output direction is as follows:

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

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

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

The following describes each field in the log in details:

1. Priority

The priority is calculated using the following formula: Facility x 8 + Level. Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. When the RFC5424 format is enabled, the default value of the facility field is local0 (16).

Version

According to RFC5424, the version is always 1.

Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Devices use the following uniformed timestamp format when the RFC5424 logging function is enabled:

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

The following table describes each parameter of the timestamp.

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

Sysname

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

Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which contain upper-case letters, digits, or underscores. The Mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

Structured-Data

Structured-data introduced in RFC5424 is parsed as a whole string containing parameter information. Each log may contain 0 or multiple parameters. If a parameter is null, replace this parameter with a placeholder (-). The format of this field is as follows:

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

The following table describes each parameter of the structured-data field.

Parameter in structured-data	Description	Remarks
SD_ID	Parameter information name	The parameter information name is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is added only to the customized parameter information, not to the parameter information defined in RFC5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). Networks' enterprise ID is 4881. You can query the enterprise ID on the official website of IANA. http://www.iana.org/assignments/enterprise-numbers
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured-data of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address or MAC address must be capitalized, and other types of values are capitalized as required.

description

This field indicates the content of the syslog.

Overview

Feature	Description
Logging	Enable or disable the system logging functions.
Syslog Format	Configure the syslog format.
Logging Direction	Configure the parameters to send syslogs in different directions.
Syslog Filtering	Configure parameters of the syslog filtering function.
Featured Logging	Configure parameters of the featured logging function.
Syslog Monitoring	Configure parameters of the syslog monitoring function.

6.3.1 Logging

Enable or disable the logging, log redirection, and log statistics functions.

Related Configuration

Enable Logging

By default, logging is enabled.

Run the **logging on** command to enable logging in global configuration mode. After logging is enabled, logs generated by the system are sent in various directions for the administrator to monitor the performance of the system.

Enabling Log Statistics

By default, log statistics is disabled.

Run the **logging count** command to enable log statistics in global configuration mode. After log statistics is enabled, the system records the number of times a log is generated and the last time when the log is generated.

6.3.2 Syslog Format

Configure the syslog format, including the RFC5424 log format, timestamp format, sysname, and sequence number.

Related Configuration

Enabling the RFC5424 Log Format

By default, the RFC5424 log format is disabled.

After the new format (RFC5424 log format) is enabled, the **service sequence-numbers, service sysname, service timestamps**, **service private-syslog**, and **service standard-syslog** that are applicable only to the old format (RFC3164 log format) lose effect and are hidden.

After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuring the Timestamp Format

By default, the syslog uses the datetime timestamp format, and the timestamp does not contain the year and millisecond.

Run the **service timestamps** command in global configuration mode to use the datetime timestamp format that contains the year and millisecond in the syslog, or change the datetime format to the uptime format.

Adding Sysname to the Syslog

By default, the syslog does not contain sysname.

Run the **service sysname** command in global configuration mode to add sysname to the syslog.

Adding the Sequence Number to the Syslog

By default, the syslog does not contain the sequence number.

Run the **service sequence-numbers** command in global configuration mode to add the sequence number to the syslog.

Enabling the Standard Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service standard-syslog** command in global configuration mode to enable the standard log format and logs are displayed in the following format:

```
timestamp %module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

Enabling the Private Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service private-syslog** command in global configuration mode to enable the private log format and logs are displayed in the following format:

```
timestamp module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing at the end of the module name in the private log format.

6.3.3 Logging Direction

Configure parameters for sending syslogs in different directions, including the Console, monitor terminal, buffer, the log server, and log files.

Related Configuration

Synchronizing User Input with Log Output

By default, this function is disabled.

Run the **logging synchronous** command in line configuration mode to synchronize user input with log output. After this function is enabled, user input will not be interrupted.

Configuring the Log Rate Limit

By default, no log rate limit is configured.

Run the **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]] command in global configuration mode to configure the log rate limit.

Configuring the Level of Logs Sent to the Console

By default, the level of logs sent to the Console is debugging (Level 7).

Run the **logging console** [*level*] command in global configuration mode to configure the level of logs that can be sent to the Console.

Sending Logs to the Monitor Terminal

By default, it is not allowed to send logs to the monitor terminal.

Run the **terminal monitor** command in the privileged EXEC mode to send logs to the monitor terminal.

Configuring the Level of Logs Sent to the Monitor Terminal

By default, the level of logs sent to the monitor terminal is debugging (Level 7).

Run the **logging monitor** [*level*] command in global configuration mode to configure the level of logs that can be sent to the monitor terminal.

Writing Logs into the Memory Buffer

By default, logs are written into the memory buffer, and the default level of logs is debugging (Level 7).

Run the **logging buffered** [*buffer-size*] [*level*] command in global configuration mode to configure parameters for writing logs into the memory buffer, including the buffer size and log level.

Sending Logs to the Log Server

By default, logs are not sent to the log server.

Run the **logging server** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*] command in global configuration mode to send logs to a specified log server.

Configuring the Level of Logs Sent to the Log Server

By default, the level of logs sent to the log server is informational (Level 6).

Run the **logging trap** [*level*] command in global configuration mode to configure the level of logs that can be sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

If the RFC5424 log format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 log format is enabled, the facility value of logs sent to the log server is local0 (16) by default.

Run the **logging facility** *facility-type* command in global configuration mode to configure the facility value of logs sent to the log server.

Configuring the Source Address of Logs Sent to the Log Server

By default, the source address of logs sent to the log server is the IP address of the interface sending logs.

Run the **logging source** [**interface**] *interface-type interface-number* command to configure the source interface of logs. If this source interface is not configured, or the IP address is not configured for this source interface, the source address of logs is the IP address of the interface sending logs.

Run the **logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address of logs. If this IP address is not configured on the device, the source address of logs is the IP address of the interface sending logs.

Writing Logs into Log Files

By default, logs are not written into log files. After the function of writing logs into log files is enabled, the level of logs written into log files is informational (Level 6) by default.

Run the **logging file** {**flash:***filename* } [*max-file-size*] [level] command in global configuration mode to configure parameters for writing logs into log files, including the type of device where the file is stored, file name, file size, and log level.

Configuring the Number of Log Files

By default, the number of log files is 16.

Run the **logging file numbers** *numbers* command in global configuration mode to configure the number of log files.

Configuring the Interval at Which Logs Are Written into Log Files

By default, logs are written into log files at the interval of 3600s (one hour).

Run the **logging flash interval** *seconds* command in global configuration mode to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

By default, the storage time is not configured.

Run the **logging life-time level** *level days* command in global configuration mode to configure the storage time of logs. The administrator can specify different storage days for logs of different levels.

Immediately Writing Logs in the Buffer into Log Files

By default, syslogs are stored in the syslog buffer and then written into log files periodically or when the buffer is full.

Run the **logging flash flush** command in global configuration mode to immediately write logs in the buffer into log files so that you can collect logs conveniently.

6.3.4 Syslog Filtering

By default, logs generated by the system are sent in all directions.

Working Principle

Filtering Direction

Five log filtering directions are defined:

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

The four filtering directions can be used either in combinations to filter out logs sent in various directions, or separately to filter out logs sent in a single direction.

Filtering Mode

Two filtering modes are available:

- **contains-only**: Indicates that only logs that contain keywords specified in the filtering rules are output. You may be interested in only a specified type of logs. In this case, you can apply the contains-only mode on the device to display only logs that match filtering rules on the terminal, helping you check whether any event occurs.
- **filter-only**: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be output. If a module generates too many logs, spamming may occur on the terminal interface. If you do not care about this type of logs, you can apply the filter-only mode and configure related filtering rules to filter out logs that may cause spamming.

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

Filter Rule

Two filtering rules are available:

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

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

Related Configuration

Configuring the Log Filtering Direction

By default, the log filtering direction is all, that is, logs sent in all directions are filtered.

Run the **logging filter direction** { **all** | **buffer | file** | **server | terminal** } command in global configuration mode to configure the log filtering direction to filter out logs in the specified directions.

↘ Configuring the Log Filtering Mode

By default, the log filtering mode is filter-only.

Run the **logging filter type** { **contains-only** | **filter-only** } command in global configuration mode to configure the log filtering mode.

↘ Configuring the Log Filtering Rule

By default, no log filtering rule is configured on a device, that is, logs are not filtered out.

Run the **logging filter rule exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* command in global configuration mode to configure the exact-match rule.

Run the **logging filter rule single-match** { **level** *level* **| mnemonic** *mnemonic-name* | **module** *module-name* } command in global configuration mode to configure the single-match rule.

6.3.5 Syslog Monitoring

After syslog monitoring is enabled, the system monitors the access attempts of users and generates the related logs.

Working Principle

After logging of login/exit attempts is enabled, the system records the access attempts of users. The log contains user name and source address.

After logging of operations is enabled, the system records changes in device configurations, The log contains user name, source address, and operation.

Related Configuration

↘ Enabling Logging of Login or Exit Attempts

By default, a device generates logs when users access or exit the device.

Run the **logging userinfo** command in global configuration mode to enable logging of login/exit attempts. After this function is enabled, the device displays logs when users access the devices through Telnet, SSH, or HTTP so that the administrator can monitor the device connections.

↘ Enabling Logging of Operations

By default, a device generates logs when users modify device configurations.

Run the **logging userinfo command-log** command in global configuration mode to enable logging of operations. After this function is enabled, the system displays related logs to notify the administrator of configuration changes.

6.4 Configuration

Configuration	Description and Command	
Configuring Syslog Format	(Optional) It is used to configure the syslog format.	
	service timestamps [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	Configures the timestamp format of syslogs.
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
	service log-format rfc5424	Enables the RFC5424 syslog format.
Sending Syslogs to the Console	(Optional) It is used to configure parameters for sending syslogs to the Console.	
	logging on	Enables logging.
	logging count	Enables log statistics.
	logging console [*level*]	Configures the level of logs displayed on the Console.
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	(Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [*level*]	Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	(Optional) It is used to configure parameters for writing syslogs into the memory buffer.	
	logging buffered [*buffer-size*] [*level*]	Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log Server	(Optional) It is used to configure parameters for sending syslogs to the log server.	
	logging server { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]	Sends logs to a specified log server.
	logging trap [*level*]	Configures the level of logs sent to the log server.
	logging facility *facility-type*	Configures the facility value of logs sent to the log server.
	logging source [**interface**] *interface-type interface-number*	Configures the source interface of logs sent to the log server.

Configuration	Description and Command	
	logging source { **ip** *ip-address* | **ipv6** *ipv6-address* }	Configures the source address of logs sent to the log server.
Writing Syslogs into Log Files	(Optional) It is used to configure parameters for writing syslogs into a file.	
	logging file { **flash:***filename* } [*max-file-size*] [level]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging file numbers *numbers*	Configures the number of files which logs are written into. The default value is 16.
	logging flash interval *seconds*	Configures the interval at which logs are written into log files. The default value is 3600.
	logging life-time level *level days*	Configures the storage time of log files.
Configuring Syslog Filtering	(Optional) It is used to enable the syslog filtering function.	
	logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }	Configures the log filtering direction.
	logging filter type { **contains-only** | **filter-only** }	Configures the log filtering mode.
	logging filter rule exact-match module *module-name* **mnemonic** *mnemonic-name* **level** *level*	Configures the exact-match filtering rule.
	logging filter rule single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }	Configures the single-match filtering rule.
Configuring Level-based Logging	(Optional) It is used to configure logging policies to send the syslogs based on module and severity level .	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	Sends logs to different destinations by module and severity level
Configuring Delayed Logging	(Optional) It is used to enable the delayed logging function.	
	logging delay-send terminal	Enables delayed display of logs on the Console and remote terminal.
	logging delay-send file flash:*filename*	Configures the name of the file on the local device where logs are buffered.
	logging delay-send interval *seconds*	Configures the interval at which logs are sent to the log server.

Configuration	Description and Command	
	logging delay-send server { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }	Configures the server address and delayed logging mode.
Configuring Periodical Logging	(Optional) It is used to enable the periodical logging function.	
	logging statistic enable	Enables the periodical logging function .
	logging statistic terminal	Enables periodical display of logs on the Console and remote terminal.
	logging statistic mnemonic *mnemonic* **interval** *minutes*	Configures the interval at which logs of a performance statistic object are sent to the server .
Configuring Syslog Redirection	(Optional) It is used to enable the log redirection function.	
	logging rd on	Enables the log redirection function.
	logging rd rate-limit *number* [**except** *severity*]	Configures the log redirection rate limit.
Configuring Syslog Monitoring	(Optional) It is used to configure parameters of the syslog monitoring function .	
	logging userinfo	Enables logging of login/exit attempts.
	logging userinfo command-log	Enables logging of operations.
Synchronizing User Input with Log Output	(Optional) It is used to synchronize the user input with log output.	
	logging synchronous	Synchronizes user input with log output.

6.4.1 Configuring Syslog Format

Configuration Effect

- Configure the format of syslogs.

Notes

RFC3164 Log Format

- If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.
- The log sequence number is a 6-digit integer. Each time a log is generated, the sequence number increases by one. Each time the sequence number increases from 000000 to 1,000,000, or reaches 2^32, the sequence number starts from 000000 again.

RFC5424 Log Format

- After the RFC5424 log format is enabled, the timestamp is uniform.

- 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.

Configuration Steps

Configuring the Timestamp Format of Syslogs

- (Optional) By default, the datetime timestamp format is used.
- Unless otherwise specified, perform this configuration on the device to configure the timestamp format.

Adding the Sysname to the Syslog

- (Optional) By default, the syslog does not contain the sysname.
- Unless otherwise specified, perform this configuration on the device to add the sysname to the syslog.

Adding the Sequence Number to the Syslog

- (Optional) By default, the syslog does not contain the sequence number.
- Unless otherwise specified, perform this configuration on the device to add the sequence number to the syslog.

Enabling the Standard Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the standard log format.

Enabling the Private Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the private log format.

Enabling the RFC5424 Log Format

- (Optional) By default, the RFC5424 log format is disabled.
- Unless otherwise specified, perform this configuration on the device to enable the RFC5424 log format.

Verification

- Generate a syslog, and check the log format.

Related Commands

Configuring the Timestamp Format of Syslogs

Command	**service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]
Parameter Description	*message-type*: Indicates the log type. There are two log types: log and debug. **uptime**: Indicates the device startup time in the format of dd:hh:mm:ss, for example, 07:00:10:41. **datetime**: Indicates the current device time in the format of MM DD hh:mm:ss, for example, Jul 27 16:53:07. **msec**: Indicates that the current device time contains millisecond.

	year: Indicates that the current device time contains year.
Command Mode	Global configuration mode
Configuration Usage	Two syslog timestamp formats are available, namely, uptime and datetime. You can select a timestamp format as required.

Adding the Sysname to the Syslog

Command	**service sysname**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sysname to the log to enable you to learn about the device that sends syslogs to the server.

Adding the Sequence Number to the Syslog

Command	**service sequence-numbers**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sequence number to the log. The sequence number starts from 1. After the sequence number is added, you can learn clearly whether any log is lost and the generation sequence of logs.

Enabling the Standard Syslog Format

Command	**service standard-syslog**
Parameter Description	N/A
Command Mode	Global configuration mode

Configuration Usage	By default, logs are displayed in the following format (default format):
	`*timestamp: %module-level-mnemonic: content`
	If the standard syslog format is enabled, logs are displayed in the following format:
	`timestamp %module-level-mnemonic: content`
	Compared with the default format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

Enabling the Private Syslog Format

Command	service private-syslog
Parameter Description	N/A
Command Mode	Global configuration mode

Configuration Usage	By default, logs are displayed in the following format (default format):
	`*timestamp: %module-level-mnemonic: content`
	If the private syslog format is enabled, logs are displayed in the following format:
	`timestamp module-level-mnemonic: content`
	Compared with the default format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing in front of the module name in the private log format.

Enabling the RFC5424 Syslog Format

Command	service log-format rfc5424
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After the new format (RFC5424 log format) is enabled, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable only to the old format (RFC3164 log format) loss effect and are hidden. After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuration Example

Enabling the RFC3164 Log Format

Scenario	It is required to configure the timestamp format as follows: 1. Enable the RFC3164 format. 2. Change the timestamp format to datetime and add the millisecond and year to the timestamp. 3. Add the sysname to the log. 4. Add the sequence number to the log.
Configuration Steps	● Configure the syslog format.

	`Hostname# configure terminal`
	`Hostname(config)# no service log-format rfc5424`
	`Hostname(config)# service timestamps log datetime year msec`

	Hostname(config)# service timestamps debug datetime year msec Hostname(config)# service sysname Hostname(config)# service sequence-numbers
Verification	After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the timestamp in the new log.
	Hostname(config)#exit 001302: *Jun 14 2013 19:01:40.293: Hostname %SYS-5-CONFIG_I: Configured from console by admin on console Hostname#show logging config Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail

↘ Enabling the RFC5424 Log Format

Scenario	It is required to enable the RFC5424 format.
Configuration Steps	● Configure the syslog format.
	Hostname# configure terminal Hostname(config)# service log-format rfc5424
Verification	Verify that new syslogs are displayed in the RFC5424 format. ● Run the **show logging config** command to display the configuration.

	● Enter or exit global configuration mode to generate a new log, and check the format of the new log.
	Hostname(config)#exit <133>1 2013-07-24T12:19:33.130290Z testSYS 5 CONFIG - Configured from console by console Hostname#show logging config Syslog logging: enabled Console logging: level debugging, 4740 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 4745 messages logged Statistic log messages: disable Statistic log messages to terminal: disable Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds Count log messages: enable Trap logging: level informational, 2641 message lines logged,4155 fail logging to 192.168.23.89 logging to 2000::1

6.4.2 Sending Syslogs to the Console

Configuration Effect

- Send syslogs to the Console to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the Console.

Configuration Steps

↘ Enabling Logging

- (Optional) By default, the logging function is enabled.

↘ Enabling Log Statistics

- (Optional) By default, log statistics is disabled.
- Unless otherwise specified, perform this configuration on the device to enable log statistics.

↘ Configuring the Level of Logs Displayed on the Console

- (Optional) By default, the level of logs displayed on the Console is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the Console.

Configuring the Log Rate Limit

- (Optional) By default, the no rate limit is configured.
- Unless otherwise specified, perform this configuration on the device to limit the log rate.

Verification

- Run the **show logging config** command to display the level of logs displayed on the Console.

Related Commands

Enabling Logging

Command	**logging on**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logging is enabled. Do not disable logging in general cases. If too many syslogs are generated, you can configure log levels to reduce the number of logs.

Enabling Log Statistics

Command	**logging count**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, log statistics is disabled. If log statistics is enabled, syslogs will be classified and counted. The system records the number of times a log is generated and the last time when the log is generated.

Configuring the Level of Logs Displayed on the Console

Command	**logging console** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs 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 displayed on the Console.

Configuring the Log Rate Limit

Command	**logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number*} } [**except** [*severity*]]
Parameter Description	*number*: Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000. **all**: Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7. **console**: Indicates the number of logs displayed on the Console per second. **except** *severity*: Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configuration Usage	By default, no rate limit is configured.

Configuration Example

Sending Syslogs to the Console

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configuration Steps	● Configure parameters for displaying syslogs on the Console.

	`Hostname# configure terminal`
	`Hostname(config)# logging count`
	`Hostname(config)# logging console informational`
	`Hostname(config)# logging rate-limit console 50`

Verification	● Run the **show logging config** command to display the configuration.

	`Hostname(config)#show logging config`
	`Syslog logging: enabled`
	`  Console logging: level informational, 1303 messages logged`
	`  Monitor logging: level debugging, 0 messages logged`
	`  Buffer logging: level debugging, 1303 messages logged`
	`  File logging: level informational, 118 messages logged`
	`  File name:syslog_test.txt, size 128 Kbytes, have written 5 files`
	`  Standard format:false`
	`  Timestamp debug messages: datetime`
	`  Timestamp log messages: datetime`

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configuration Steps	● Configure parameters for displaying syslogs on the Console.

	`Hostname# configure terminal`
	`Hostname(config)# logging count`
	`Hostname(config)# logging console informational`
	`Hostname(config)# logging rate-limit console 50`

Verification	● Run the **show logging config** command to display the configuration.

	`Sequence-number log messages: enable`
	`Sysname log messages: enable`
	`Count log messages: enable`
	`Trap logging: level informational, 118 message lines logged,0 fail`

6.4.3 Sending Syslogs to the Monitor Terminal

Configuration Effect

- Send syslogs to a remote monitor terminal to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the monitor terminal.
- By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs.

Configuration Steps

↘ Allowing the Monitor Terminal to Display Logs

- (Mandatory) By default, the monitor terminal is not allowed to display logs.
- Unless otherwise specified, perform this operation on every monitor terminal connected to the device.

↘ Configuring the Level of Logs Displayed on the Monitor Terminal

- (Optional) By default, the level of logs displayed on the monitor terminal is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the monitor terminal.

Verification

- Run the **show logging config** command to display the level of logs displayed on the monitor terminal.

Related Commands

Allowing the Monitor Terminal to Display Logs

Command	**terminal monitor**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Configuration Usage	By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs.

Configuring the Level of Logs Displayed on the Monitor Terminal

Command	**logging monitor** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the monitor terminal is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs displayed on the monitor terminal.

Configuration Example

Sending Syslogs to the Monitor Terminal

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	● Configure parameters for displaying syslogs on the monitor terminal.

	`Hostname# configure terminal`
	`Hostname(config)# logging monitor informational`
	`Hostname(config)# line vty 0 4`
	`Hostname(config-line)# monitor`

Verification	● Run the **show logging config** command to display the configuration.
	`Hostname#show logging config`

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Displaylogs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	● Configure parameters for displaying syslogs on the monitor terminal.
	Hostname# configure terminal Hostname(config)# logging monitor informational Hostname(config)# line vty 0 4 Hostname(config-line)# monitor
Verification	● Run the **show logging config** command to displaythe configuration.
	Syslog logging: enabled Console logging: level informational, 1304 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level debugging, 1304 messages logged File logging: level informational, 119 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 119 message lines logged,0 fail

Common Errors

- To disable this function, run the **terminal no monitor** command, instead of the **no terminal monitor** command.

6.4.4 Writing Syslogs into the Memory Buffer

Configuration Effect

- Write syslogs into the memory buffer so that the administrator can view recent syslogs by running the **show logging** command.

Notes

- If the buffer is full, old logs will be overwritten by new logs that are written into the memorybuffer.

Configuration Steps

Writing Logs into the Memory Buffer

- (Optional) By default, the system writes logs into the memory buffer, and the default level of logs is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to write logs into the memory buffer.

Verification

- Run the **show logging config** command to display the level of logs written into the memory buffer.
- Run the **show logging** command to display the level of logs written into the memory buffer.

Related Commands

Writing Logs into the Memory Buffer

Command	**logging buffered** [*buffer-size*] [*level*]
Parameter Description	*buffer-size*: Indicates the size of the memory buffer. *level*: Indicates the level of logs that can be written into the memory buffer.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs written into the memory buffer is debugging (Level 7). Run the **show logging** command in privileged EXEC mode to display the level of logs written into the memory buffer and the buffer size.

Configuration Example

Writing Syslogs into the Memory Buffer

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	● Configure parameters for writing syslogs into the memory buffer.
	`Hostname# configure terminal` `Hostname(config)# logging buffered 131072 informational`
Verification	● Run the **show logging config** command to display the configuration and recent syslogs.

	`Hostname#show logging`
	`Syslog logging: enabled`
	`  Console logging: level informational, 1306 messages logged`
	`  Monitor logging: level informational, 0 messages logged`
	`  Buffer logging: level informational, 1306 messages logged`

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	● Configure parameters for writing syslogs into the memory buffer.
	Hostname# configure terminal Hostname(config)# logging buffered 131072 informational
Verification	● Run the **show logging config** command to display the configuration and recent syslogs.
	File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail Log Buffer (Total 131072 Bytes): have written 4200 001301: *Jun 14 2013 19:01:09.488: Hostname %SYS-5-CONFIG_I: Configured from console by admin on console 001302: *Jun 14 2013 19:01:40.293: Hostname %SYS-5-CONFIG_I: Configured from console by admin on console //Logs displayed are subject to the actual output of the **show logging** command.

6.4.5 Sending Syslogs to the Log Server

Configuration Effect

- Send syslogs to the log server to facilitate the administrator to monitor logs on the server.

Notes

- To send logs to the log server, you must add the timestamp and sequence number to logs. Otherwise, the logs are not sent to the log server.

Configuration Steps

↘ Sending Logs to a Specified Log Server

- (Mandatory) By default, syslogs are not sent to any log server.

- Unless otherwise specified, perform this configuration on every device.

Configuring the Level of Logs Sent to the Log Server

- (Optional) By default, the level of logs sent to the log server is informational (Level 6).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

- (Optional) If the RFC5424 format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the log server is local0 (16) by default.
- Unless otherwise specified, perform this configuration on the device to configure the facility value of logs sent to the log server.

Configuring the Source Interface of Logs Sent to the Log Server

- (Optional) By default, the source interface of logs sent to the log server is the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source interface of logs sent to the log server.

Configuring the Source Address of Logs Sent to the Log Server

- (Optional) By default, the source address of logs sent to the log server is the IP address of the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source address of logs sent to the log server.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

Sending Logs to a Specified Log Server

Command	**logging server** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*] Or **logging** { *ip-address* | **ipv6** *ipv6-address* } [**udp-prot** *port*]
Parameter Description	*ip-address*: Specifies the IP address of the host that receives logs. **ipv6** *ipv6-address*: Specifies the IPv6 address of the host that receives logs. **udp-port** *port*: Specifies the port ID of the log server. The default port ID is 514.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs will be sent simultaneously to all these log servers. You can configure up to five log servers on a product.

Configuring the Level of Logs Sent to the Log Server

Command	**logging trap** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs sent to the log server is informational (Level 6). You can run the **show logging config** command in privileged EXEC mode to display the level of logs sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

Command	**logging facility** *facility-type*
Parameter Description	*facility-type*: Indicates the facility value of logs.
Command Mode	Global configuration mode
Configuration Usage	If the RFC5424 format is disabled, the facility value of logs sent to the server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the server is local0 (16) by default.

Configuring the Source Interface of Logs Sent to the Log Server

Command	**logging source** [**interface**] *interface-type interface-number*
Parameter Description	*interface-type*: Indicates the interface type. *interface-number*: Indicates the interface number.
Command Mode	Global configuration mode
Configuration Usage	By default, the source interface of logs sent to the log server is the interface sending the logs. To facilitate management, you can use this command to set the source interface of all logs to an interface so that the administrator can identify the device that sends the logs based on the unique address.

Configuring the Source Address of Logs Sent to the Log Server

Command	**logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* }
Parameter Description	**ip** *ip-address*: Specifies the source IPv4 address of logs sent to the IPv4 log server. **ipv6** *ipv6-address*: Specifies the source IPv6 address of logs sent to the IPv6 log server.
Command Mode	Global configuration mode
Configuration Usage	By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs. To facilitate management, you can use this command to set the source IP address of all logs to the IP address of an interface so that the administrator can identify the device that sends the logs based on the unique address..

Configuration Example

Sending Syslogs to the Log Server

Scenario	It is required to configure the function of sending syslogs to the log server as follows: 1. Set the IPv4 address of the log server to 10.1.1.100. 2. Set the level of logs that can be sent to the log server to debugging (Level 7). 3. Set the source interface to Loopback 0.
Configuration Steps	● Configure parameters for sending syslogs to the log server.
	Hostname# configure terminal Hostname(config)# logging server 10.1.1.100 Hostname(config)# logging trap debugging Hostname(config)# logging source interface Loopback 0
Verification	● Run the **show logging config** command to display the configuration.
	Hostname#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level informational, 122 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false 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, 122 message lines logged,0 fail logging to 10.1.1.100

6.4.6 Writing Syslogs into Log Files

Configuration Effect

- Write syslogs into log files at the specified interval so that the administrator can view history logs anytime on the local device.

Notes

- Sylsogs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at the interval of one hour by default) or when the buffer is full.

Configuration Steps

Writing Logs into Log Files

- (Mandatory) By default, syslogs are not written to any log file.
- Unless otherwise specified, perform this configuration on every device.

Configuring the Number of Log Files

- (Optional) By default, syslogs are written to 16 log files.
- Unless otherwise specified, perform this configuration on the device to configure the number of files which logs are written into.

Configuring the Interval at Which Logs Are Written into Log Files

- (Optional) By default, syslogs are written to log files every hour.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

- (Optional) By default, no storage time is configured.
- Unless otherwise specified, perform this configuration on the device to configure the storage time of log files.

Immediately Writing Logs in the Buffer into Log Files

- (Optional) By default, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full.
- Unless otherwise specified, perform this configuration to write logs in the buffer into log files immediately. This command takes effect only once after it is configured.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

Writing Logs into Log Files

Command	**logging file** { **flash:***filename* } [*max-file-size*] [*level*]
Parameter Description	**flash**: Indicates that log files will be stored on the extended Flash. *filename*: Indicates the log file name, which does not contain a file name extension. The file name extension is always txt. *max-file-size*: Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default

	value is 128 KB. *level*: Indicates the level of logs that can be written into a log file.
Command Mode	Global configuration mode
Configuration Usage	This command is used to create a log file with the specified file name on the specified file storage device. The file size increases with the amount of logs, but cannot exceed the configured maximum size. If not specified, the maximum size of a log file is 128 KB by default. After this command is configured, the system saves logs to log files. A log file name does not contain any file name extension. The file name extension is always txt, which cannot be changed. After this command is configured, logs will be written into log files every hour. If you run the **logging flie flash:syslog** command, a total of 16 log files will be created, namely, **syslog.txt**, **syslog_1.txt**, **syslog_2.txt**, …, **syslog_14.txt**, and **syslog_15.txt**. Logs are written into the 16 log files in sequence. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is full. When **syslog_15.txt** is full, logs are written into **syslog.txt** again,

Configuring the Number of Log Files

Command	**logging file numbers** *numbers*
Parameter Description	*numbers*: Indicates the number of log files. The value ranges from 2 to 32.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the number of log files. If the number of log files is modified, the system will not delete the log files that have been generated. Therefore, you need to manually delete the existing log files to save the space of the extended flash. (Before deleting existing log files, you can transfer these log files to an external server through TFTP.) For example, after the function of writing logs into log files is enabled, 16 log files will be created by default. If the device has generated 16 log files and you change the number of log files to 2, new logs will be written into **syslog.txt** and **syslog_1.txt** by turns. The existing log files from **syslog_2.txt** to **syslog_15.txt** will be preserved. You can manually delete these log files.

Configuring the Interval at Which Logs Are Written into Log Files

Command	**logging flash interval** *seconds*
Parameter Description	*seconds*: Indicates the interval at which logs are written into log files. The value ranges from 1 s to 51,840 s.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the interval at which logs are written into log files. The countdown starts after the command is configured.

Configuring the Storage Time of Log Files

Command	**logging life-time level** *level days*

Parameter Description	*level*: Indicates the log level. *days*: Indicates the storage time of log files. The unit is day. The storage time is not less than seven days.
Command Mode	Global configuration mode
Configuration Usage	After the log storage time is configured, 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** is the absolute time of the day when the logs are generated, **filename** is the log file named configured by the **logging file flash** command, and **level** is the log level. After you specify the storage time for logs of a certain level, the system deletes the logs after the storage time expires. Currently, the storage time ranges from 7days to 365 days. If the log storage time is not configured, logs are stored based on the file size to ensure compatibility with old configuration commands.

Immediately Writing Logs in the Buffer into Log Files

Command	**logging flash flush**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After this command is configured, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full. You can run this command to immediately write logs into log files. ⚠ The **logging flash flush** command takes effect once after it is configured. That is, after this command is configured, logs in the buffer are immediately written to log files.

Configuration Example

Writing Syslogs into Log Files

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.

	`Hostname# configure terminal`
	`Hostname(config)# logging file flash:syslog debugging`
	`Hostname(config)# logging flash interval 600`

Verification	● Run the **show logging config** command to display the configuration.
	`Hostname(config)#show logging config`

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.
	Hostname# configure terminal Hostname(config)# logging file flash:syslog debugging Hostname(config)# logging flash interval 600
Verification	● Run the **show logging config** command to display the configuration.
	Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level debugging, 122 messages logged File name:syslog.txt, size 128 Kbytes, have written 1 files Standard format:false 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, 122 message lines logged,0 fail logging to 10.1.1.100

6.4.7 Configuring Syslog Filtering

Configuration Effect

- Filter out a specified type of syslogs if the administrator does not want to display these syslogs.
- By default, logs generated by all modules are displayed on the Console or other terminals. You can configure log filtering rules to display only desired logs.

Notes

- Two filtering modes are available: contains-only and filter-only. You can configure only one filtering mode at a time.

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

Configuration Steps

Configuring the Log Filtering Direction

- (Optional) By default, the filtering direction is all, that is, all logs are filtered out.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering direction.

Configuring the Log Filtering Mode

- (Optional) By default, the log filtering mode is filter-only.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering mode.

Configuring the Log Filtering Rule

- (Mandatory) By default, no filtering rule is configured.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering rule.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Configuring the Log Filtering Direction

Command	**logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }
Parameter Description	**all**: Filters out all logs. **buffer**: Filters out logs sent to the log buffer, that is, the logs displayed by the **show logging** command. **file**: Filters out logs written into log files. **server**: Filters out logs sent to the log server. **terminal**: Filters out logs sent to the Console and VTY terminal (including Telnet and SSH).
Command Mode	Global configuration mode
Configuration Usage	The default filtering direction is **all**, that is, all logs are filtered out. Run the **default logging filter direction** command to restore the default filtering direction.

Configuring the Log Filtering Mode

Command	**logging filter type** { **contains-only** | **filter-only** }
Parameter Description	**contains-only**: Indicates that only logs that contain keywords specified in the filtering rules are displayed. **filter-only**: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be displayed.
Command Mode	Global configuration mode

Configuration Usage	Log filtering modes include contains-only and filter-only. The default filtering mode is filter-only.

Configuring the Log Filtering Rule

Command	**logging filter rule** { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }}
Parameter Description	**exact-match**: If exact-match is selected, you must specify all three filtering options. **single-match**: If single-match is selected, you may specify only one of the three filtering options. **module** *module-name*: Indicates the module name. Logs of this module will be filtered out. **mnemonic** *mnemonic-name*: Indicates the mnemonic. Logs with this mnemonic will be filtered out. **level** *level*: Indicates the log level. Logs of this level will be filtered out.
Command Mode	Global configuration mode
Configuration Usage	Log filtering rules include exact-match and single-match. The **no logging filter rule exact-match** [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*] command is used to delete the exact-match filtering rules. You can delete all exact-match filtering rules at a time or one by one. The **no logging filter rule single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] command is used to delete the single-match filtering rules. You can delete all single-match filtering rules at a time or one by one.

Configuration Example

Configuring Syslog Filtering

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to **terminal** and **server.** 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	● Configure the syslog filtering function.

	`Hostname# configure terminal`
	`Hostname(config)# logging filter direction server`
	`Hostname(config)# logging filter direction terminal`
	`Hostname(config)# logging filter type filter-only`
	`Hostname(config)# logging filter rule single-match module SYS`

Verification	● Run the **show running-config | include loggging** command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	`Hostname#configure`

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to **terminal** and **server.** 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	● Configure the syslog filtering function.
	Hostname# configure terminal Hostname(config)# logging filter direction server Hostname(config)# logging filter direction terminal Hostname(config)# logging filter type filter-only Hostname(config)# logging filter rule single-match module SYS
Verification	● Run the **show running-config | include loggging** command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#exit Hostname# Hostname#show running-config | include logging logging filter direction server logging filter direction terminal logging filter rule single-match module SYS

6.4.8 Configuring Syslog Monitoring

Configuration Effect

- Record login/exit attempts. After logging of login/exit attempts is enabled, the related logs are displayed on the device when users access the device through Telnet or SSH. This helps the administrator monitor the device connections.
- Record modification of device configurations. After logging of operations is enabled, the related logs are displayed on the device when users modify the device configurations. This helps the administrator monitor the changes in device configurations.

Notes

- If both the **logging userinfo** command and the **logging userinfo command-log** command are configured on the device, only the configuration result of the **logging userinfo command-log** command is displayed when you run the **show running-config** command.

- If both the **logging userinfo** configuration and the **logging userinfo command-log** configuration are disabled on the device, only the configuration result of the **no logging userinfo** command is displayed when you run the **show running-config** command.

Configuration Steps

Enabling Logging of Login/Exit Attempts

- (Optional) By default, logging of login/exit attempts is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of login/exit attempts.

Enabling logging of Operations

- (Optional) By default, logging of operations is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of operations.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Enabling Logging of Login/Exit Attempts

Command	**logging userinfo**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, a device generates related logs when users log into or exit the device.

Enabling Logging of Operations

Command	**logging userinfo command-log**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	The system generates related logs when users run configuration commands. By default, a device generates logs when users modify device configurations.

Configuration Example

Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	● Configure the syslog monitoring function.
	Hostname# configure terminal Hostname(config)# logging userinfo Hostname(config)# logging userinfo command-log
Verification	● Run the **show running-config | include logging** command to display the configuration. ● Run a command in global configuration mode, and verify that the system generates a log.
	Hostname#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#interface gigabitEthernet 0/0 *Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface GigabitEthernet 0/0 Hostname#show running-config | include logging logging userinfo command-log

6.4.9 Synchronizing User Input with Log Output

Configuration Effect

- By default, the user input is not synchronized with the log output. After this function is enabled, the content input during log output is displayed after log output is completed, ensuring integrity and continuity of the input.

Notes

- This command is executed in line configuration mode. You need to configure this command on every line as required.

Configuration Steps

↘ **Synchronizing User Input with Log Output**

- (Optional) By default, the synchronization function is disabled.
- Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

- Run the **show running** command to display the configuration.

Related Commands

↘ **Synchronizing User Input with Log Output**

Command	logging synchronous
Parameter Description	N/A
Command Mode	Line configuration mode
Configuration Usage	This command is used to synchronize the user input with log output to prevent interrupting the user input.

Configuration Example

Synchronizing User Input with Log Output

Scenario	It is required to synchronize the user input with log output as follows: 1. Enable the synchronization function.
Configuration Steps	● Configure the synchronization function.
	Hostname# configure terminal Hostname(config)# line console 0 Hostname(config-line)# logging synchronous
Verification	● Run the **show running-config | begin line** command to display the configuration.
	Hostname#show running-config | begin line line con 0 logging synchronous login local As shown in the following output, when a user types in "vlan", the state of interface 0/1 changes and the related log is output. After log output is completed, the log module automatically displays the user input "vlan" so that the user can continue typing. Hostname(config)#vlan *Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up *Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up Hostname(config)#vlan

6.5 Monitoring

Clearing

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

Description	Command
Clears logs in the memory buffer.	**clear logging**

Displaying

Description	Command
Displays log statistics and logs in the memory buffer based on the timestamp from oldest to latest.	**show logging**
Displays log statistics and logs in the memory buffer based on the timestamp from latest to oldest.	**show logging reverse**
Displays syslog configurations and statistics.	**show logging config**
Displays log statistics of each module in the system.	**show logging count**

7 Configuring Security Logs

7.1 Overview

SECURITY-LOG (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.

Key operations:

(1) Adding/deleting accounts

(2) Editing authentication information

(3) Modifying configurations (such as a DNS address and an IP address)

(4) User login/logout

(5) Restarting/Stopping the device

(6) Uploading/downloading files (when supported)

(7) Editing user permissions (when supported)

(8) Enabling/disabling log auditing and deleting logs

Protocols and Standards

- N/A

7.2 Applications

Application	Description
Enabling the Secuirty Log Auditing Function	A network administrator need to check recent key operations on a device. When an abnormal operation occurs on the device (for example, a key configuration is tampered), the administrator can find who performed the operation and when and how the user did it.

7.2.1 Enabling the Security Log Auditing Function

Scenario

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 loging in to the device, the administrator can view records to check the users who accessed the device and whether they perform key operations such as modifying device configurations.

Figure 7-1



Remarks	The administrator log in to the device to check the logs recording kep operations on the device.

Deployment

- Enable the function directly to use it.

7.3 Features

Basic Concepts

Key Operations

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. The default log storage time is 180 days. (The storage time is configurable.)

Features

Feature	Description
Enabling the Secuirty Log Auditing Function	Enable the security log auditing function to record key operations on a device.

7.3.1 Enabling the Security Log Auditing Function

You can enable the security log auditing function to record key operations on a device and save logs locally.

Working Principle

After the security log auditing function is enabled, when a user performs a key operation, such as account management, login/logout, system restart, configuration file change, and enabling or disabling log auditing function, the corresponding service module collects information, such as the 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.

The logs of key operations are stored for 180 days by default. The storage time is configurable. By default, the system checks whether any local logs have exceeded the storage time at 03:00:00 every day and deletes expired logs. The handling time is configurable.

A maximum of 10,000 logs can be stored by default. The storage capacity can be adjusted from 500 to 10,000. New logs overwrite earliest logs if the number of stored logs exceeds the storage capacity.

Related Configuration

Enabling the Security Log Auditing Function

By default, the function is disabled.

7.4 Configuration

Configuration	Description and Command	
Enabling the Security Log Auditing Function	Mandatory.	
	security-log audit-enable	Enables the security log auditing function.
Configuring the Local Storage Time of Security Logs	Optional.	
	security-log data-store-days *day*	Configures the local storage time of security logs.
Configuring the Handling Time of Aging Security Logs	Optional.	
	security-log auto-vacuum-time *hh:mm:ss*	Configures the handling time of aging security logs.
Configuring the Local Storage Capacity for Security Logs	Optional.	
	security-log data-store-items *num*	Configures the local storage capacity for security logs.

7.4.1 Enabling the Security Log Auditing Function

Configuration Effect

- 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, and write the logs to its local database.

Notes

- N/A

Configuration Steps

Enabling the Security Log Auditing Function

- Mandatory.
- Enable the function on the device.

Verification

- Log in to the device, perform a key operation and check security logs.

Related Commands

Enabling the Security Log Auditing Function

Command	security-log audit-enable
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	• Enable the security log auditing function.
	Hostname# configure terminal Hostname(config)# security-log audit-enable
Verification	An authorized user logs in to the device and performs a key operation. Check security logs after 30 seconds.
	Hostname# show security-log detail all time, username, peerinfo, hostname, log-type: content 2019-10-22 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG: SECURITY_LOG deleted all security log successfully 2019-10-22 10:00:02, admin, vty0(192.168.111.111), Hostname, SEC_LOG: SECURITY_LOG disabled security log audit configuration unsuccessfully 2019-10-22 10:00:03, ---, console, Hostname, SEC_LOG: SECURITY_LOG enabled security log audit configuration successfully ……

Common Errors

- N/A

7.4.2 Configuring the Local Storage Time of Security Logs

Configuration Effect

- After the local storage time of security logs is configured, expired logs will be deleted.

Notes

- N/A

Configuration Steps

Configuring the Local Storage Time of Security Logs

- Optional.
- Security logs are stored for 180 days by default. The value range of storage time is from 1 to 65535.

Verification

- Run the **show running-config** command or the **show security-log config** command to display configuration status.

Related Commands

Configuring the Local Storage Time for Security Logs

Command	**security-log data-store-days** *day*
Parameter Description	*day:* the number of days. The value range is from 1 to 65535. The default range is 180.
Command Mode	Global configuration mode.
Usage Guide	Configure the local storage time of security logs. Expired logs will be cleared.

Configuration Example

Configuration Steps	● Set the local storage time of security logs to 300 days.
	`Hostname# configure terminal` `Hostname(config)# security-log data-store-days 300`
Verification	Run the **show running-config** command or the **show security-log config** command to display configuration status.

	`Hostname# show running | in security-log data-store-days`
	`security-log data-store-days 300`
	
	`Hostname# show security-log config`
	`Security-log audit: enable`
	`Limit number: 10000`
	`Store days: 300`
	`Auto vacuum time: 03:00:00`

Common Errors

- N/A

7.4.3 Configuring the Handling Time of Aging Security Logs

Configuration Effect

After the handling time of aging 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.

Notes

- N/A

Configuration Steps

Configuring the Handling Time of Aging Security Logs

- Optional.
- By default, the system handles the aging security logs at 03:00:00 everyday.

Verification

- Run the **show running-config** command or the **show security-log config** command to display configuration status.

Related Commands

Configuring the Handling Time of Aging Security Logs

Command	**security-log auto-vacuum-time** *hh:mm:ss*
Parameter Description	*hh:mm:ss:* hour:minute:second. The default time is 03:00:00.
Command Mode	Global configuration mode.
Usage Guide	Configure the handling time of aging security logs, the system checks whether any logs have exceeded the storage time at the configured handling time (deviation: 5 minutes) and deletes expired logs..

Configuration Example

Configuration Steps	● Set the handling time of aging security logs to 05:05:00 every day.
	`Hostname# configure terminal` `Hostname(config)# security-log auto-vacuum-time 05:05:00`
Verification	Run the **show running-config** command or the **show security-log config** command to display configuration status.

	`Hostname# show running | in security-log auto-vacuum-time`
	`security-log auto-vacuum-time 05:05:00`
	
	`Hostname# show security-log config`
	`Security-log audit: enable`
	`Limit number: 10000`
	`Store days: 300`
	`Auto vacuum time: 05:05:00`

Common Errors

- N/A

7.4.4 Configuring the Local Storage Capacity for Security Logs

Configuration Effect

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 capacity.

Notes

- N/A

Configuration Steps

↘ Configuring the Local Storage Capacity for Security Logs

- Optional.
- The default value and the maximum value for the local storage capacity depends on the device capacity. The value range of the capacity is from 500 to 10,000. The default value is 10,000 and the minimum value is 500 which is required by safety standards.

Verification

- Run the **show running-config** command or the **show security-log config** command to display configuration status.

Related Commands

↘ Configuring the the Local Storage Capacity for Security Logs

Command	**security-log data-store-items** *num*
Parameter Description	● *num:* the local storage capacity for security logs. The default value and the maximum value for the local storage capacity depends on the device capacity. The value range of the capacity is from 500 to 10,000. The default value is 10,000 and the minimum value is 500 which is required by safety standards.
Command Mode	Global configuration mode.
Usage Guide	If flash space is limited, you can run this command to decrease the storage capacity for security logs.

Configuration Example

Configuration Steps	● Set the local storage capacity for security logs to 1000.
	`Hostname# configure terminal`

	`Hostname(config)# security-log data-store-items 1000`
Verification	Run the **show running-config** command or the **show security-log config** command to display configuration status.

	`Hostname# show running | in security-log data-store-items`
	`security-log data-store-items 1000`
	
	`Hostname# show security-log config`
	`Security-log audit: enable`
	`Limit number: 1000`
	`Store days: 300`
	`Auto vacuum time: 05:05:00`

Common Errors

- N/A

7.5 Monitoring

Clearing

Description	Command
Clears all logs.	**security-log delete all**

Displaying

Description	Command
Display all logs.	**show security-log**
Displays detailed log information, which can be filtered by time, log type, username, host name, and terminal information.	**show security-log detail** { **all** | { **from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* } } [**log-type** { **SEC_LOG** | **ACC_MNT** | **LOGIN** | **SYS** | **CONFIG** | **OTHER** }] [**user** *username*] [**hostname** *hostname*] [**peerinfo** *peerinfo*] **{** [**order-by** [**time** | **log-type**] { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]] **}**
Exports detailed log information, which can be filtered by time, log type, username, host name, and terminal information.	**show security-log detail export** { **from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* } [**log-type** { **SEC_LOG** | **ACC_MNT** | **LOGIN** | **SYS** | **CONFIG** | **OTHER** }] [**user** *username*] [**hostname** *hostname*] [**peername** *peername*] [**ip** *ip-address*]
Displays the count of logs, which can be filtered by time, log type, username, host name, and terminal information.	**show security-log detail stat** { **all |** { **from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* } } [**log-type** { **SEC_LOG** | **ACC_MNT** | **LOGIN** | **SYS** | **CONFIG** | **OTHER** }] [**user** *username*] [**hostname** *hostname*] [**peerinfo** *peerinfo*]
Displays log configurations.	**show security-log config**

Displays log statistics.	**show security-log statistics**
Displays statistics during log processing.	**show security-log info**

Debugging

System resources are occupied when debugging information is output. Disable the debugging function immediately after use.

Description	Command
Debugs log auditing.	**debug security-log errors**
Debugs received logs.	**debug security-log recv-info**
Debugs the log database.	**debug security-log sql-info**

8 Configuring CWMP

8.1 Overview

CPE WAN Management Protocol (CWMP) provides a general framework of unified device management, related message specifications, management methods, and data models, so as to solve difficulties in unified management and maintenance of dispersed customer-premises equipment (CPEs), improve troubleshooting efficiency, and save O&M costs.

CWMP provides the following functions:

- **Auto configuration and dynamic service provisioning.** CWMP allows an Auto-Configuration Server (ACS) to automatically provision CPEs who initially access the network after start. The ACS can also dynamically re-configure running CPEs.
- **Firmware management.** CWMP manages and upgrades the firmware and its files of CPEs.
- **Software module management.** CWMP manages modular software according to data models implemented.
- **Status and performance monitoring.** CWMP enables CPEs to notify the ACE of its status and changes, achieving real-time status and performance monitoring.
- **Diagnostics.** The ACE diagnoses or resolves connectivity or service problems based on information from CPEs, and can also perform defined diagnosis tests.

Protocols and Standards

For details about TR069 protocol specifications, visit http://www.broadband-forum.org/technical/trlist.php.

Listed below are some major CWMP protocol specifications:

- TR-069_Amendment-4.pdf: CWMP standard
- TR-098_Amendment-2.pdf: Standard for Internet gateway device data model
- TR-106_Amendment-6.pdf: Standard for CPE data model
- TR-181_Issue-2_Amendment-5.pdf: Standard for CPE data model 2
- tr-098-1-4-full.xml: Definition of Internet gateway device data model
- tr-181-2-4-full.xml: Definition 2 of CPE data model 2

8.2 Applications

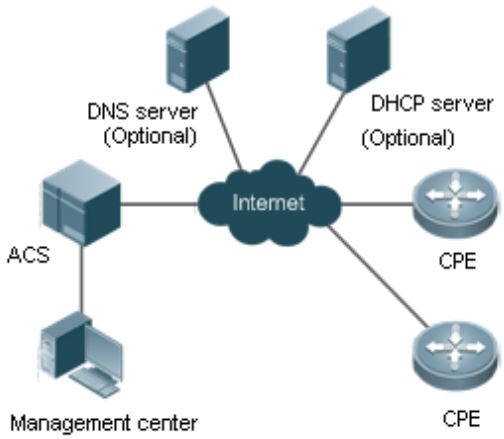
Typical Application	Scenario
CWMP Network Application Scenario	Initiate CPE-ACS connection, so as to upgrade the CPE firmware, upload the configuration files, restore the configuration, and realize other features.

8.2.1 CWMP Network Application Scenario

Application Scenario

The major components of a CWMP network architecture are CPEs, an ACS, a management center, a DHCP server, and a Domain Name System (DNS) server. The management center manages a population of CPEs by controlling the ACS on a Web browser.

Figure 7-1



Note	● If the Uniform Resource Locator (URL) of the ACS is configured on CPEs, the DHCP server is optional. If not, the DHCP is required to dynamically discover the ACS URL. ● If the URLs of the ACS and CPEs contain IP addresses only, the DNS server is optional. If their URLs contain domain names, the DNS server is required to resolves the names.

Functional Deployment

HTTP runs on both CPEs and the ACS.

8.3 Features

Basic Concept

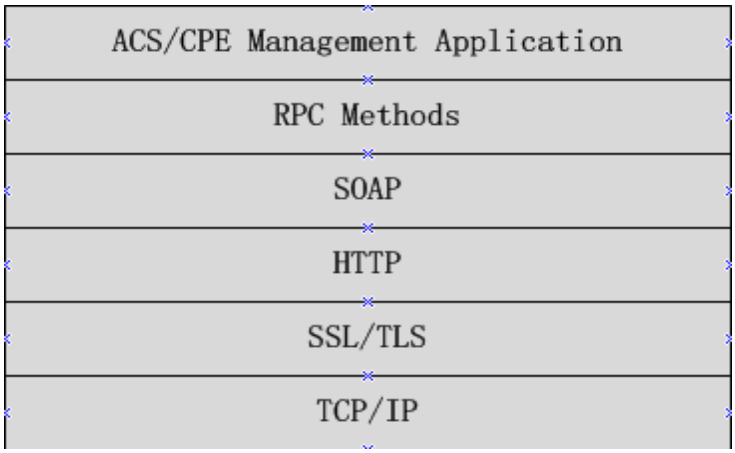
↘ Major Terminologies

- **CPE**: Customer Premises Equipment
- **ACS**: Auto-Configuration Server
- **RPC**: Remote Procedure Call
- **DM**: Data Model

Protocol Stack

Figure 7-2 shows the protocol stack of CWMP.

Figure 7-2 CWMP Protocol Stack



As shown in Figure 7-2, CWMP defines six layers with respective functions as follows:

- ACS/CPE Application

The application layer is not a part of CWMP. It is the development performed by various modules of the CPEs/ACS to support CWMP, just like the Simple Network Management Protocol (SNMP), which does not cover the MIB management of functional modules.

- RPC Methods

This layer provides various RPC methods for interactions between the ACS and the CPEs.

- SOAP

The Simple Object Access Protocol (SOAP) layer uses a XML-based syntax to encode and decode CWMP messages.. Thus, CWMP messages must comply with the XML-based syntax.

- HTTP

All CWMP messages are transmitted over Hypertext Transfer Protocol (HTTP). Both the ACS and the CPEs can behave in the role of HTTP clients and servers. The server function 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) protocol stack.

RPC Methods

The ACS manages and monitors CPEs by calling mostly the following RPC methods:

- Get RPC Methods

The Get methods enable the ACS to remotely obtain the set of RPC methods, as well as names, values and attributes of the DM parameters supported on CPEs.

- Set RPC Methods

The Set methods enable the ACS to remotely set the values and attributes of the DM parameters supported on CPEs.

- Inform RPC Methods

The Inform methods enable CPEs to inform the ACS of their device identifiers, parameter information, and events whenever sessions are established between them.

- Download RPC Methods

The Download method enables the ACS to remotely control the file download of CPEs, including firmware management, upgrade, and Web package upgrade.

- Upload RPC Methods

The Upload method enables the ACS to remotely control the file upload of CPEs, including upload of firmware and logs.

- Reboot RPC Methods

The Reboot method enables the ACS to remotely reboot the CPEs.

Session Management

CWMP sessions or interactions are the basis for CWMP. All CWMP interactions between the ACS and CPEs rely on their sessions. CWMP helps initiate and maintain ACS-CPE sessions to link them up for effective management and monitoring. An ACS-CPE session is a TCP connection, which starts from the Inform negotiation to TCP disconnection. The session is classified into CPE Initiated Session and ACS Initiated Session according to the session poster.

DM Management

CWMP operates based on CWMP Data Model (DM). CWMP manages all functional modules by a set of operations performed on DM. Each functional module registers and implements a respective data model, just like the MIBs implemented by various functional modules of SNMP.

A CWMP data model is represented in the form of a character string. For a clear hierarchy of the data model, a dot (.) is used as a delimiter to distinguish an upper-level data model node from a lower-level data model node. For instance, in the data model **InternetGatewayDevice.LANDevice**, **InternetGatewayDevice** is the parent data model node of **LANDevice**, and **LANDevice** is the child data model node of **InternetGatewayDevice**.

DM nodes are classified into two types: object nodes and parameter nodes. The parameter nodes are also known as leaf nodes. An object node is a node under which there are child nodes, and a parameter node is a leaf node under which there is no any child node. Object nodes are further classified into single-instance object nodes and multi-instance object nodes. A single-instance object node is an object node for which there is only one instance, whereas a multi-instance object node is an object node for which there are multiple instances.

A data model node has two attributes. One attribute relates to a notification function; that is, whether to inform the ACS of changes (other than changes caused by CWMP) to parameter values of the data model. The other attribute is an identifier indicating that the parameters of the data model node can be written using other management modes (than the ACS); that is,

whether the values of the parameters can be modified using other management modes such as Telnet. The ACS can modify the attributes of the data models using RPC methods.

CWMP manages the data models using corresponding RPC methods.

↘ Event Management

When some events concerned by the ACS occur on the CPE, the CPE will inform the ACS of these events. The ACS monitors these events to monitor the working status of the CPE. The CWMP events are just like Trap messages of SNMP or product logs. Using RPC methods, to the ACS filters out the unconcerned types of events. CWMP events are classified into two types: single or (not cumulative) events and multiple (cumulative) events. A single event means that there is no quantitative change to the same event upon re-occurrence of the event, with the old discarded and the newest kept. A multiple event means that the old are not discarded and the newest event is kept as a complete event when an event re-occurs for multiple times later; that is, the number of this event is incremented by 1.

All events that occur on the CPE are notified to the ACS using the INFORM method.

Features

Feature	Description
Upgrading the Firmware	The ACS controls the upgrade of the firmware of a CPE using the Download method.
Upgrading the Configuration Files	The ACS controls the upgrade of the configuration files of a CPE using the Download method.
Uploading the Configuration Files	The ACS controls the upload of the configuration files of a CPE using the Upload method.
Backing up and Restoring a CPE	When a CPE breaks away from the management center, this feature can remotely restore the CPE to the previous status.

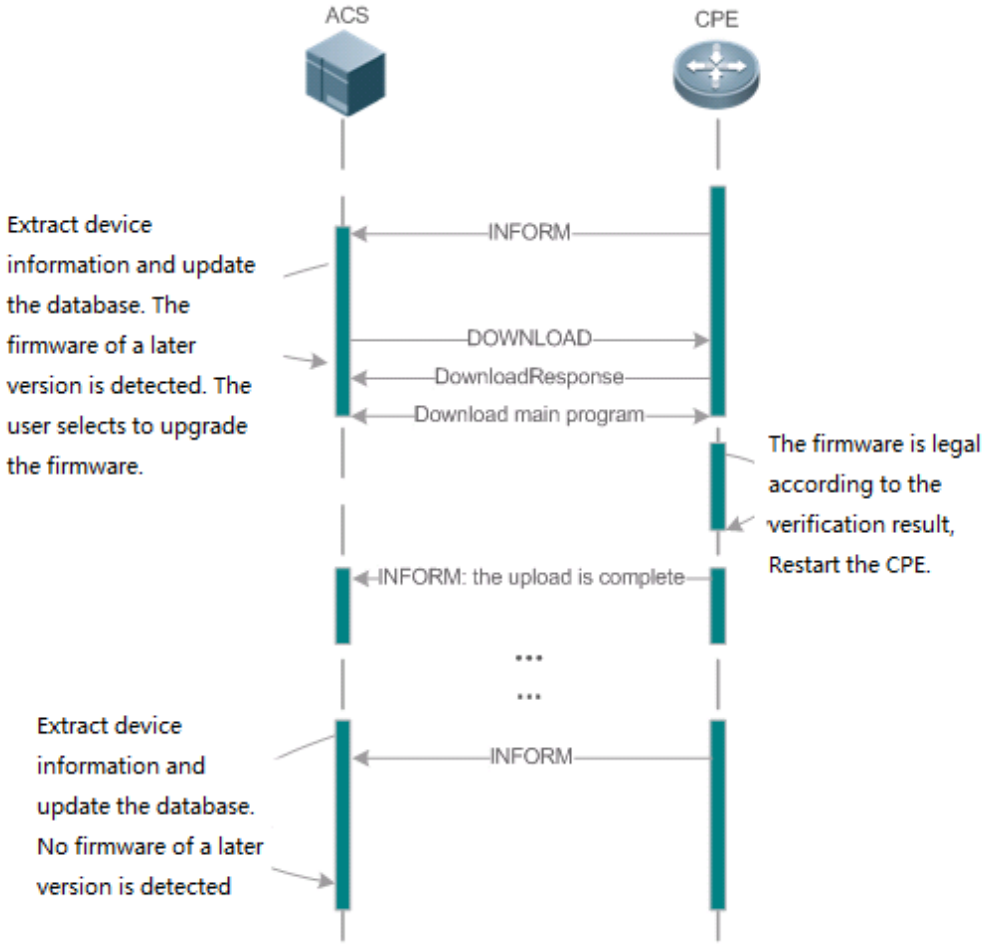
8.3.1 Upgrading the Firmware

Upgrading the Firmware means the firmware of a network element (NE) can be upgraded, so as to implement device version upgrade or replacement.

Working Principle

↘ Sequence Diagram of Upgrading the Firmware

Figure 7-3



Users specify a CPE for the ACS to deliver the Download method for upgrading the firmware. The CPE receives the request and starts to download the latest firmware from the destination file server, upgrade the firmware, and then reboot. After restart, the CPE will indicate the successful or unsuccessful completion of the method application.

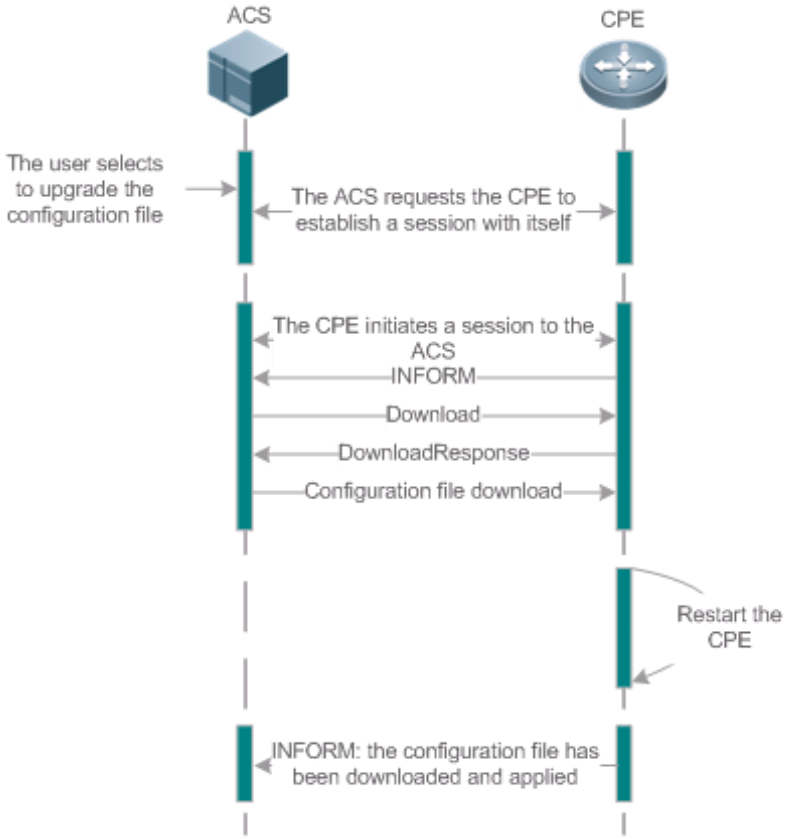
The file server can be ACS or separately deployed.

8.3.2 Upgrading the Configuration Files

Upgrading the Configuration Files means the current configuration files of a CPE can be replaced with specified configuration files, so that the new configuration files act on the CPE after reset.

Working Principle

Figure 7-4



Users specify a CPE for the ACS to deliver the Download methods for upgrading its configuration files. The CPE downloads the configuration files from the specified file server, upgrade configuration files, and then reboot. After that, the CPE will indicate successful or unsuccessful completion of the method application.

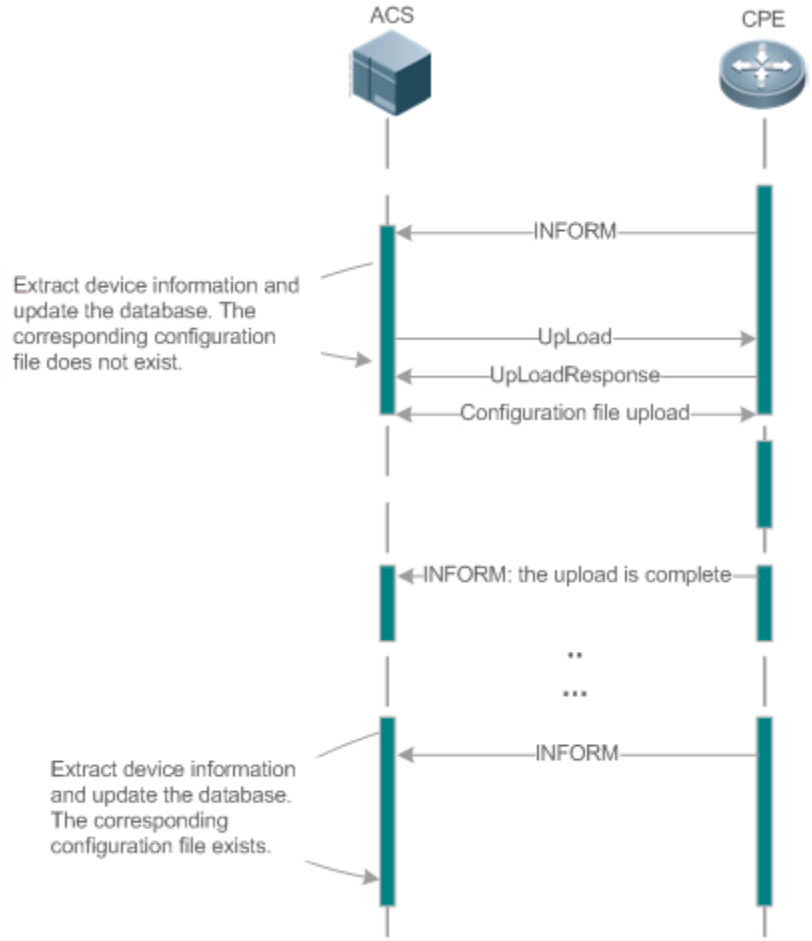
The file server can be ACS or separately deployed.

8.3.3 Uploading the Configuration Files

Uploading the Configuration Files means the ACS controls the configuration files of CPEs by using the Upload method.

Working Principle

Figure 7-5



When a CPE initially accesses the ACS, the ACS attempts to learn the configuration files of the CPE in the following sequence:

- When the ACS initially receives an Inform message from the CPE, it locates the corresponding database information according to device information carried in the message.
- If the database does not contain the configuration files of the CPE, the ACS delivers the Upload method to the CPE for uploading the configuration files.
- The CPE uploads its current configuration files to the ACS.
- The CPE returns a successful or unsuccessful response to the Upload request.

8.3.4 Backing Up and Restoring a CPE

When a remote CPE breaks away from the management center due to abnormal operations, the CPE backup and restoration feature helps restore the CPE to the previous status, so that the management center can resume the supervision of the CPE as necessary.

Working Principle

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its firmware or configuration files. Then when the CPE fails to connect to the ACS and breaks away from the management center after its firmware or configuration files are upgraded, the previous firmware or configuration files of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong version or configuration file.

Before the CPE receives a new firmware or configuration files to upgrade, the CPE will back up its current version and configuration files. In addition, there is a mechanism for determining whether the problem described in the preceding scenario has occurred. If the problem has occurred, the CPE is restored to the previous manageable status.

8.4 Configuration

Action	Suggestions and Related Commands	
Establishing a Basic CWMP Connection	⚠ (Mandatory) You can configure the ACS or CPE usernames and passwords to be authenticated for CWMP connection.	
	cwmp	Enables CWMP and enters CWMP configuration mode.
	acs username	Configures the ACS username for CWMP connection.
	acs password	Configures the ACS password for CWMP connection.
	cpe username	Configures the CPE username for CWMP connection.
	cpe password	Configures the CPE password for CWMP connection.
	⚠ (Optional) You can configure the URLs of the CPE and the ACS.	
	acs url	Configures the ACS URL.
	cpe url	Configures the CPE URL.
Configuring CWMP-Related Attributes	⚠ (Optional) You can configure the basic functions of the CPE, such as upload, backup and restoration of firmware, configuration files or logs.	
	cpe inform	Configures the periodic notification function of the CPE.
	cpe back-up	Configures the backup and restoration of the firmware and configuration file of the CPE.
	disable download	Disables the function of downloading firmware and configuration files from the ACS.

Action	Suggestions and Related Commands	
	disable upload	Disables the function of uploading configuration and log files to the ACS.
	timer cpe- timeout	Configures the ACS response timeout on CPEs.

8.4.1 Establishing a Basic CWMP Connection

Configuration Effect

- A session connection is established between the ACS and the CPE.

Precautions

- N/A

Configuration Method

Enabling CWMP and Entering CWMP Configuration Mode

- (Mandatory) The CWMP function is enabled by default.

Command	**cwmp**
Parameter Description	N/A
Defaults	CWMP is enabled by default.
Command Mode	Global configuration guide
Usage Guide	N/A

Configuring the ACS Username for CWMP Connection

- This configuration is mandatory on the ACS.
- Only one username can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs username** *username*
Parameter Description	**username** *username*: The ACS username for CWMP connection
Defaults	The ACS username is not configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Password for CWMP Connection

- This configuration is mandatory on the ACS.

- The password of the ACS can be in plaintext or encrypted form. Only one password can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password:* ACS password *encryption-type:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-type*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Username for CWMP Connection

- This configuration is mandatory on the CPE.
- Only one username can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe username** *username*
Parameter Description	*username*: CPE username
Defaults	No CPE username is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Password for CWMP Connection

- This configuration is mandatory on the CPE.
- The password of the CPE can be in plaintext or encrypted form. Only one password can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password:* CPE password *encryption-type:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-type*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

	● Contain 1 to 26 characters including letters and figures. ● The leading spaces will be ignored, while the trailing and middle are valid. ● If 7 (simple encryption) is specified, the valid characters only include 0 to 9 and a (A) to f (F).

Configuring the ACS URL for CMWP Connection

- This configuration is optional on the CPE.
- Only one ACS URL can be configured. If multiple are configured, the latest configuration is applied. The ACS URL must be in HTTP format.

Command	**acs url** { *url* | **macc** }
Parameter Description	*url*: ACS URL **macc**: MACC.
Defaults	No ACS URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If the ACS URL is not configured but obtained through DHCP, CPEs will use this dynamic URL to initiate connection to the ACS. The ACS URL must: ● Be in format of **http://host[:port]/path** or **https://host[:port]/path**. ● Contain 256 characters at most. Use this command to connect to MACC quickly, achieving the same effect of running the following two commands: ● acs url https://cloud.ruijie.com.cn/service/acs ● cpe inform interval 30

Configuring the CPE URL for CWMP Connection

- This configuration is optional on the CPE.
- Only one CPE URL can be configured. If multiple are configured, the latest configuration is applied. The CPE URL must be in HTTP format instead of domain name format.

Command	**cpe url** *url*
Parameter Description	*url:* CPE URL
Defaults	No CPE URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If CPE URL is not configured, it is obtained through DHCP. The CPE URL must: ● Be in format of **http://ip** [: **port**]/. ● Contain 256 characters at most.

Verification

- Run the **show cwmp configuration** command.

Command	**show cwmp configuration**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Examples	The following example displays the CWMP configuration.
	`Hostname(config-cwmp)#show cwmp configuration`
	`CWMP Status : enable`
	`ACS URL : http://www.ruijie.com.cn/acs`
	`ACS username : admin`
	`ACS password : ******`
	`CPE URL : http://10.10.10.2:7547/`
	`CPE username : Hostname`
	`CPE password : ******`
	`CPE inform status : disable`
	`CPE inform interval : 60s`
	`CPE inform start time : 0:0:0 0 0 0`
	`CPE wait timeout : 50s`
	`CPE download status : enable`
	`CPE upload status : enable`
	`CPE back up status : enable`
	`CPE back up delay time : 60s`

Configuration Examples

The following configuration examples describe CWMP-related configuration only.

Configuring Usernames and Passwords on the CPE

Network Environment Figure 7-6	
Configuration Method	● Enable CWMP. ● On the CPE, configure the ACS username and password to be authenticated for the CPE to connect to the ACS. ● On the CPE, configure the CPE username and password to be authenticated for the ACS to connect to

	the CPE.
CPE	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# cwmp Hostname(config-cwmp)# acs username USERB Hostname(config-cwmp)# acs password PASSWORDB Hostname(config-cwmp)# cpe username USERB Hostname(config-cwmp)# cpe password PASSWORDB
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfullyapplied.
CPE	Hostname # show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : USERB CPE password : ******

↘ Configuring the URLs of the ACS and the CPE

Network Environment	See Figure 1-6
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.
CPE	Hostname# configure terminal Hostname(config)# cwmp Hostname(config-cwmp)# acs url http://10.10.10.1:7547/acs Hostname(config-cwmp)# cpe url http://10.10.10.1:7547/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfullyapplied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs

Network Environment	See Figure 1-6
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.
CPE	Hostname# configure terminal Hostname(config)# cwmp Hostname(config-cwmp)# acs url http://10.10.10.1:7547/acs Hostname(config-cwmp)# cpe url http://10.10.10.1:7547/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
	ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/

Common Errors

- The user-input encrypted password is longer than 254 characters, or the length of the password is not an even number.
- The user-input plaintext password is longer than 100 characters.
- The user-input plaintext password contains illegal characters.
- The user-input encrypted password contains illegal characters (the legitimate characters includes only 0~9, a~f and A~F)
- The URL of the ACS is set to **NULL**.
- The URL of the CPE is set to **NULL**.

8.4.2 Configuring CWMP-Related Attributes

Configuration Effect

- You can configure common functions of the CPE, such as the backup and restoration of its firmware or configuration file, whether to enable the CPE to download firmware and configuration files from the ACS, and whether to enable the CPE to upload its configuration and log files to the ACS.

Configuration Method

↘ Configuring the Periodic Notification Function of the CPE

- (Optional) The value range is from 30 to 3,600 in seconds. The default value is 600 seconds.
- Perform this configuration to reset the periodical notification interval of the CPE.

Command	**cpe inform** [**interval** *seconds*] [**start-time** *time*]
Parameter	*seconds*: Specifies the periodical notification interval of the CPE. The value range is from 30 to 3,600 in

Description	seconds. *time*: Specifies the date and time for starting periodical notification in *yyyy-mm-ddThh:mm:ss* format.
Command Mode	CWMP configuration mode
Defaults	The default value is 600 seconds.
Usage Guide	Use this command to configure the periodic notification function of the CPE. ● If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval. ● If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

Disabling the Function of Downloading Firmware and Configuration Files from the ACS

- (Optional) The CPE can download firmware and configuration files from the ACS by default.
- Perform this configuration if the CPE does not need to download firmware and configuration files from the ACS.

Command	**disable download**
Parameter Description	N/A
Defaults	The CPE can download firmware and configuration files from the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of downloading main program and configuration files from the ACS. ● This command does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.

Disabling the Function of Uploading Configuration and Log Files to the ACS

- (Optional.) The CPE can upload configuration and log files to the ACS by default.
- Perform this configuration if the CPE does not need to upload configuration and log files to the ACS.

Command	**disable upload**
Parameter Description	N/A
Defaults	The CPE can upload configuration and log files to the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

Configuring the Backup and Restoration of the Firmware and Configuration Files of the CPE

- (Optional) The backup and restoration of the firmware and configuration files of the CPE is enabled by default. The value range is from 30 to 10,000 in seconds. The default value is 60 seconds.
- The longer the delay-time is, the longer the reboot will be complete.
- Perform this configuration to modify the function of backing up and restoring the firmware and configuration files of the CPE.

Command	**cpe back-up [delay-time** *seconds*]
Parameter Description	*seconds*: Specifies the delay for backup and restoration of the firmware and configuration file of the CPE.
Defaults	The default value is 60 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Response Timeout

- (Optional) The value range is from 10 to 600 in seconds. The default value is 30 seconds.
- Perform this configuration to modify the ACS response timeout period on the CPE.

Command	**timer cpe- timeout** *seconds*
Parameter Description	*seconds*: Specifies the timeout period in seconds. The value range is from 10 to 600.
Defaults	The default value is 30 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Verification

- Run the show cwmp configuration command.

Command	**show cwmp configuration**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Examples	The following example displays the CWMP configuration.
	`Hostname(config-cwmp)#show cwmp configuration`
	`CWMP Status : enable`
	`ACS URL : http://www.ruijie.com.cn/acs`
	`ACS username : admin`

```
ACS password                    : ******
CPE URL                         : http://10.10.10.2:7547/
CPE username                    : Hostname
CPE password                    : ******
CPE inform status               : disable
CPE inform interval             : 60s
CPE inform start time           : 0:0:0 0 0 0
CPE wait timeout                : 50s
CPE download status             : enable
CPE upload status               : enable
CPE back up status              : enable
CPE back up delay time          : 60s
```

Configuration Examples

Configuring the Periodical Notification Interval of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval of the CPE to 60 seconds.

CPE	`Hostname#config`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#cwmp`
	`Hostname(config-cwmp)#cpe inform interval 60`

Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.

CPE	`Hostname #show cwmp configuration`
	`CWMP Status                    : enable`
	`.....`
	`CPE inform interval            : 60s`

Disabling the Function of Downloading Firmware and Configuration Files from the ACS

Network Environment	See Figure 7-6.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the function of downloading firmware and configuration files from the ACS.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)#disable download
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE download status : disable

Disabling the Function of Uploading Configuration and Log Files to the ACS

Network Environment	See Figure 7-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the CPE's function of uploading configuration and log files to the ACS.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# disable upload
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE upload status : disable

Configuring the Backup and Restoration Delay

Network Environment	See Figure 7-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 30 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# cpe back-up Seconds 30
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE back up delay time : 30s

Configuring the ACS Response Timeout of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the response timeout of the CPE to 100 seconds.
CPE	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# cwmp Hostname(config-cwmp)# timer cpe-timeout 100
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname#show cwmp configuration CWMP Status : enable ..... CPE wait timeout : 100s

Common Errors

N/A

8.5 Monitoring

Displaying

Command	Function
show cwmp configuration	Displays the CWMP configuration.
show cwmp status	Displays the CWMP running status.

9 Configuring MONITOR

9.1 Overview

Intelligent monitoring is the intelligent hardware management of Network devices, including intelligent fan speed adjustment, and intelligent temperature monitoring. The intelligent monitoring performs the following tasks:

- Automatic fan speed adjustment based on ambient temperature changes
- Real-time temperature monitoring of boards to alert users

By default, the intelligent monitoring function is enabled after the device is powered on. It does not require any manual configuration.

Protocol Specification

N/A

9.2 Features

Basic Concepts

N/A

Features

Feature	Function
Intelligent Speed Adjustment of Fans	The rotating speed of fans is automatically adjusted as the temperature changes to address the heat dissipation needs of the system.
Intelligent Temperature Monitoring	The system automatically monitors the temperature. When the temperature exceeds a certain threshold, the system automatically generates an alarm.
Power monitoring	The system automatically monitors the power. When the power is insufficient or cannot be identified, the system automatically generates an alarm.

9.2.1 Intelligent Speed Adjustment of Fans

As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

Working Principle

The system automatically specifies default start rotating speed for the fans according to the current operating mode of the fans. As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

Verification

- Run the **show fan** command to display working status of all fans.
- Run the **show fan speed command** to dislay rotating speed.

9.2.2 Intelligent Temperature Monitoring

The system automatically monitors the temperature. When the temperature changes, the system automatically notifies users.

Working Principle

The system monitors the temperature once per minute. When the temperature exceeds a certain threshold, the system takes a certain action. The temperature and action vary with different devices.

Verification

Use the **show temperature** command to check the temperature thresholds and the current temperature of each line card.

9.2.3 Run the show temperature command to display system temperature. Power Monitoring

The system automatically monitors the power. When the power is insufficient or cannot be identified, the system automatically generates an alarm.

Working Principle

The system monitors the power once per minutes. If the system finds the power insufficient, the alarm LED becomes yellow and a Syslog message is generated. Once the alarm event is resolved, the system recovers. If the system cannot identify the inserted power, the alarm LED becomes yellow. After you remove the power, the system recovers.

Verification

Run the **show power** command to display power information.

10 Configuring ZAM

10.1 Overview

Manual deployment of all required devices for go-online on a network consumes a lot of labor and material resources, and has the following problems or defects:

- Manual deployment of a massive number of devices for go-online on a network imposes a high technical requirement on deployment personnel. It requires a long period, resulting in high labor and material costs.
- Manual deployment of a massive number of devices may cause fatigue, and consequently, may easily cause deployment inconsistency or errors, resulting in network malfunction.
- Manual deployment does not support control and unified management, easily causing difference and inconsistency.
- It is hard to track an event and network device deployment. The entire deployment process cannot be controlled and easily results in problems or missing.
- It is hard to manage device go-online in a unified manner. Online statuses of devices cannot be tracked and thus administrators cannot learn about the online and running statuses of the devices on the network.
- Device extensibility is poor. Automatic deployment of extensible devices and even the extensible network is not supported.

To address the preceding problems, our company launches the ZAM solution to enable zero configuration of network devices, support plug-and-play, and realize unified and automatic deployment. The ZAM solution imposes few technical requirement on deployment personnel and helps reduce workload and costs. It avoids inconsistent deployment, supports unified deployment and management, tracks online statuses of devices, and simplifies operation, maintenance, and deployment of a massive number of devices.

Protocols and Standards

- RFC1541: DHCP standard

10.2 Application

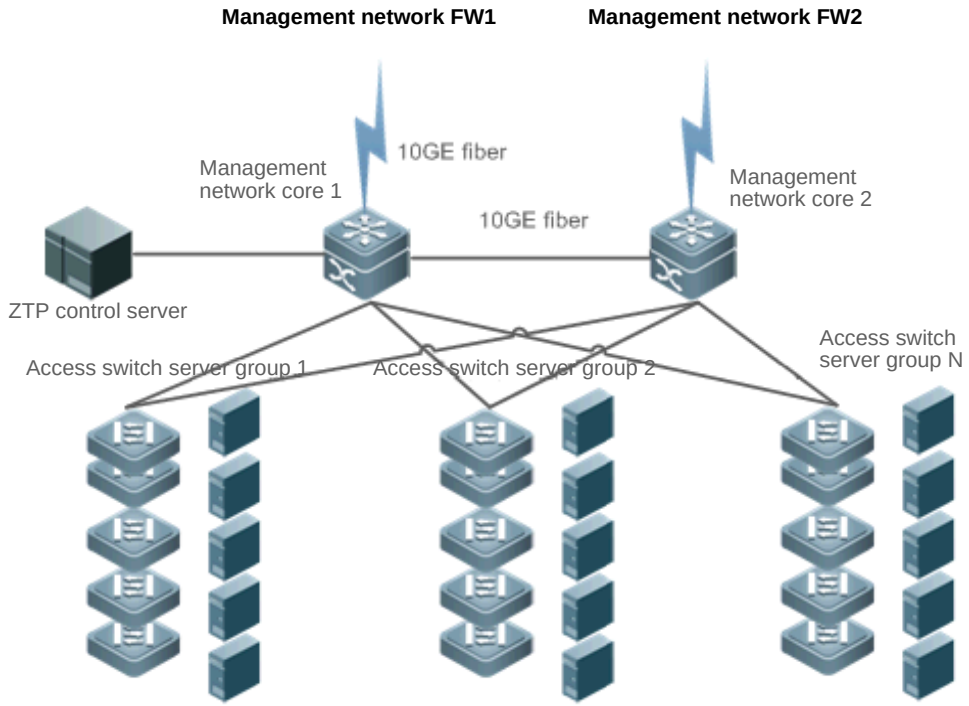
Application	Description
ZAM Automatic Deployment	Implements unified management on device deployment for go-online.

10.2.1 ZAM Automatic Deployment

Scenario

Figure 10-1 shows the network topology for ZAM solution. On the basis of the original network, a ZAM control server is added. DHCP and TFTP services are deployed on the ZAM server for managing and controlling device deployment in a unified manner for go-online, thus realizing unified management of all the deployed devices.

Figure 10-1



Deployment

- Deploy DHCP and TFTP services on the ZAM control server.
- Enable ZAM for access switch server groups 1, 2…N.

10.3 Features

Basic Concepts

ZAM

Zero Automatic Manage

IDC

Internet Data Center

DHCP

Dynamic Host Configuration Protocol

TFTP

Trivial File Transfer Protocol

Feature

Feature	Description
Device Go-online via ZAM	Uses the ZAM solution to enable zero configuration of network devices.

10.3.1 Device Go-online via ZAM

The ZAM solution is implemented via three steps.

Step 1: A device without configurations accesses a network. The device applies for a fixed IP address from the ZAM control server via DHCP. The ZAM control server responds to the application by returning an IP address and the response also carries the TFTP server IP address and the configuration file name corresponding to the device. The device automatically applies the IP address, and resolves the TFTP server IP address and the configuration file name carried in the response.

Step 2: The device downloads the corresponding configuration file from the ZAM control server via TFTP (a TFTP server can be independently established).

Step 3: The device loads the configuration file.

The ZAM control server and device requiring go-online must meet the following requirements:

The ZAM control server must:

- Be capable of identifying a device requiring go-online, IP address of a specific device, the TFTP server IP address, and configuration file name of this device saved on the TFTP server.
- Be capable of allocating IP addresses to a device requiring go-online, that is, be capable of providing the DHCP service to pre-allocate an IP address, a TFTP server IP address, and a configuration file name, and enabling matching between the device and the preceding pre-allocated information.
- Provide the TFTP function and support configuration file download and storage if the TFTP function is deployed on the ZAM control server (recommended).

The device requiring go-online must:

- Be capable of automatically determining whether to go online via the ZAM solution after being powered on, that is, determining whether to go online without configuration via the ZAM solution.
- Be capable of applying to the DHCP server for an IP address, and obtaining the TFTP server IP address and configures file name.
- Be capable of downloading the specified configuration scripts from the TFTP server via TFTP.
- Be capable of automatically loading the configuration script.
- Provide a retry mechanism upon a ZAM deployment failure and provide a ZAM exit mechanism.

Working Principle

Device go-online via ZAM is divided into four stages:

Initialization

At this stage, a device without configurations is powered on and accesses a network. After loading is completed, the device automatically pre-deploys the ZAM environment. The pre-deployment requirement is as follows:

- Use the MGMT port for ZTP management and retain all default configurations without extra operation.

DHCP

After the pre-deployment, the device obtains the ZAM management IP address, TFTP server IP address, configuration file name of the device via DHCP. Requirements are as follows:

- On the MGMT port, enable DHCP.
- Trigger DHCP to obtain the ZAM management IP address. Add request identifiers of Option 67 (boot file name) and Option 150 (TFTP server IP address) to the requested parameter list.
- Resolve and deploy ZAM management IP address. Resolve Option 67 and Option 150 in the response.

TFTP

Download the corresponding configuration script according to the configuration file name and TFTP server IP address obtained at the DHCP stage.

After the configuration script is downloaded successfully, execute the configuration script to download the corresponding configuration file or bin file from the TFTP server.

Configuration loading

Load the configuration file or bin file obtained at the TFTP stage and restart the device.

Related Configuration

Enabling ZAM

This function is enabled by default.

Run the ZAM command to enable or disable ZAM.

ZAM must be enabled on the device to implement automatic deployment via ZAM.

10.4 Configuration

Configuration	Description and Command	
Configuring ZTP Configuring Device Go-online via ZAM	⚠ (Mandatory) It is used to enable ZAM.	
	zam	Enables ZAM.

10.4.1 Configuring Device Go-online via ZAM

Configuration Effect

- Configure device go-online via ZAM, so that a device without configurations enters the go-online process and implements automatic deployment.

Notes

- Deploy a ZTP control server that supports device go-online via ZAM.

Configuration Steps

Enabling ZAM

- Mandatory.
- Enable ZAM on each switch, unless otherwise specified.

Verification

Run the **show zam** command to check whether ZAM is enabled and to check configuration of the MGMT port.

Related Commands

Enabling ZAM

Command	**zam**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure ZAM.

Configuration Example

The following configuration example describes ZAM-related configuration only.

Configuring Device Go-online via ZAM

Scenario	
Configuration Steps	Configure device go-online via ZAM as follows: ● Enable ZAM.
Online device via ZAM	A# configure terminal A(config)# zam A(config)# exit
Verification	● Run the **show zam** command to display the current configuration and status of ZAM..

Hostname	Hostname#show zam ZTP state : disable ZTP status : Now is idle ZTP manage interface: Mgmt 0 Hostname#

Common Errors

- The network connection between a device requiring go-online and the ZAM control server is abnormal.
- The device requiring go-online is not in the zero-configuration state.

10.5 Monitoring

Displaying

Description	Command
Displays the current configuration and status of ZAM.	**show zam**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging function immediately after use.

Description	Command
Debugs the ZAM framework event.	**debug zam**

11 Configuring Supervisor Module Redundancy

11.1 Overview

Supervisor module redundancy is a mechanism that adopts real-time backup (also called hot backup) of the service running status of supervisor modules to improve the device availability.

In a network device with the control plane separated from the forwarding plane, the control plane runs on a supervisor module and the forwarding plane runs on cards. The control plane information of the master supervisor module is backed up to the slave supervisor module in real time during device running. When the master supervisor module is shut down as expected (for example, due to software upgrade) or unexpectedly (for example, due to software or hardware exception), the device can automatically and rapidly switch to the slave supervisor module without losing user configuration, thereby ensuring the normal operation of the network. The forwarding plane continues with packet forwarding during switching. The forwarding is not stopped and no topology fluctuation occurs during the restart of the control plane.

The supervisor module redundancy technology provides the following conveniences for network services:

1. Improving the network availability

The supervisor module redundancy technology sustains data forwarding and the status information about user sessions during switching.

Preventing neighbors from detecting link flaps

The forwarding plane is not restarted during switching. Therefore, neighbors cannot detect the status change of a link from Down to Up.

Preventing route flaps

The forwarding plane sustains forwarding communication during switching, and the control plane rapidly constructs a new forwarding table. The process of replacing the old forwarding table with the new one is unobvious, preventing route flaps.

Preventing loss of user sessions

Thanks to real-time status synchronization, user sessions that are created prior to switching are not lost.

11.2 Applications

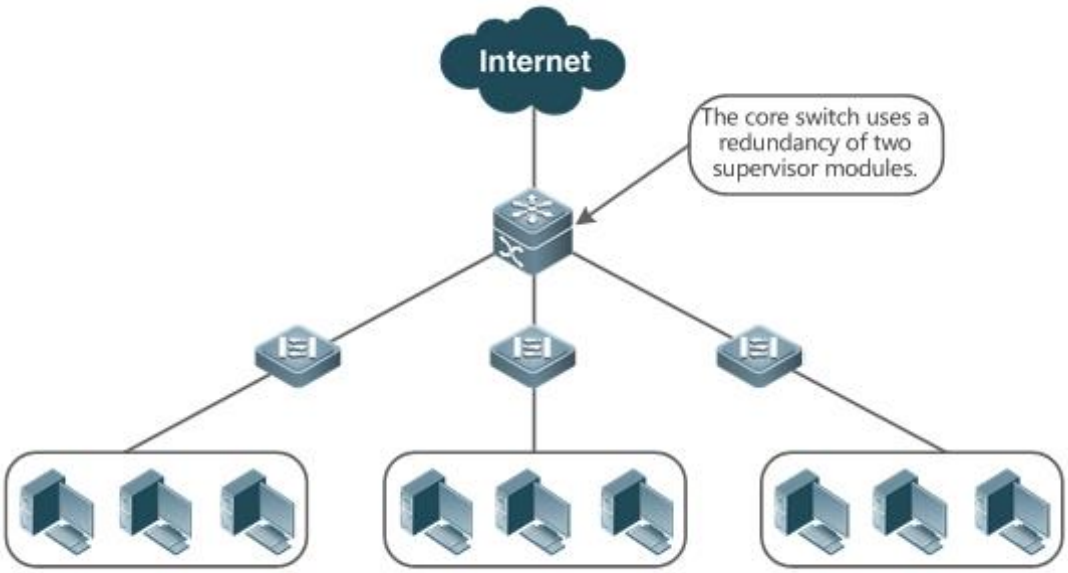
Application	Description
Redundancy of Supervisor Modules	On a core switch where two supervisor modules are installed, the redundancy technology can improve the network stability and system availability.

11.2.1 Redundancy of Supervisor Modules

Scenario

As shown in the following figure, in this network topology, if the core switch malfunctions, networks connected to the core switch break down. In order to improve the network stability, two supervisor modules need to be configured on the core switch to implement redundancy. The master supervisor module manages the entire system and the slave supervisor module backs up information about service running status of the master supervisor module in real time. When manual switching is performed or forcible switching is performed due to a failure occurring on the master supervisor module, the slave supervisor module immediately takes over functions of the master supervisor module. The forwarding plane can proceed with data forwarding and the system availability is enhanced.

Figure 11-1



Deployment

For case-type devices, each device is equivalent to one supervisor module and one line card.

11.3 Features

Basic Concepts

Master Supervisor Module, Slave Supervisor Module

On a device where two supervisor modules are installed, the system elects one supervisor module as active, which is called the master supervisor module. The other supervisor module functions as a backup supervisor module. When the master supervisor module malfunctions or actively requests switching, the backup supervisor module takes over the functions of the master supervisor module and becomes the new master supervisor module, which is called the slave supervisor module. In general, the slave supervisor module does not participate in switch management but monitors the running status of the master supervisor module.

Prerequisites for Redundancy of Supervisor Modules

In a device system, the hardware and software of all supervisor modules must be compatible so that the redundancy of supervisor modules functions properly.

Batch synchronization is required between the master and slave supervisor modules during startup so that the two supervisor modules are in the same state. The redundancy of supervisor modules is ineffective prior to synchronization.

↘ Redundancy Status of Supervisor Modules

The master supervisor module experiences the following status changes during master/slave backup:

- alone state: In this state, only one supervisor module is running in the system, or the master/slave switching is not complete, and redundancy is not established between the new master supervisor module and the new slave supervisor module.
- batch state: In this state, redundancy is established between the master and slave supervisor modules and batch backup is being performed.
- realtime state: The master supervisor module enters this state after the batch backup between the master and slave supervisor modules is complete. Real-time backup is performed between the master and slave supervisor modules, and manual switching can be performed only in this state.

Overview

Feature	Description
Information Synchronization of Supervisor Modules	In the redundancy environment of supervisor modules, the master supervisor module synchronizes status information and configuration files to the slave supervisor module in real time.

11.3.1 Information Synchronization of Supervisor Modules

Working Principle

- Status synchronization

The master supervisor module synchronizes its running status to the slave supervisor module in real time so that the slave supervisor module can take over the functions of the master supervisor module at any time, without causing any perceivable changes.

- Configuration synchronization

There are two system configuration files during device running: running-config and startup-config. running-config is a system configuration file dynamically generated during running and changes with the service configuration. startup-config is a system configuration file imported during device startup. You can run the **write** command to write running-config into startup-config or run the **copy** command to perform the copy operation.

For some functions that are not directly related to non-stop forwarding, the synchronization of system configuration files can ensure consistent user configuration during switching.

In the case of redundancy of dual supervisor modules, the master supervisor module periodically synchronizes the startup-config and running-config files to the slave supervisor module and all candidate supervisor modules. The configuration synchronization is also triggered in the following operations:

1. The running-config file is synchronized when the device switches from the global configuration mode to privileged EXEC mode.
2. The startup-config file is synchronized when the **write** or **copy** command is executed to save the configuration.
3. Information configured over the Simple Network Management Protocol (SNMP) is not automatically synchronized and the synchronization of the running-config file needs to be triggered by running commands on the CLI.

Related Configuration

- Run the **auto-sync time-period** command to adjust the interval for the master supervisor module to synchronize configuration files.

11.4 Configuration

Configuration	Description and Command	
Configuring Manual Master/Slave Switching	⚠ Optional.	
	show redundancy states	Displays the hot backup status.
Configuring the Automatic Synchronization Interval	⚠ Optional.	
	redundancy	Enters the redundancy configuration mode.
	auto-sync time-period	Configures the automatic synchronization interval of configuration files in the case of redundancy of dual supervisor modules.

11.4.1 Configuring the Automatic Synchronization Interval

Configuration Effect

Change the automatic synchronization interval of the startup-config and running-config files. If the automatic synchronization interval is set to a smaller value, changed configuration is frequently synchronized to other supervisor modules, preventing the configuration loss incurred when services and data are forcibly switched to the slave supervisor module when the master supervisor module malfunctions.

Configuration Steps

- Optional. Make the configuration when the synchronization interval needs to be changed.
- Make the configuration on the master supervisor module.

Verification

- View the output syslogs to check whether timed synchronization is performed.

Related Commands

Entering the Redundancy Configuration Mode

Command	**redundancy**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Automatic Synchronization Interval of Configuration Files

Command	**Auto-sync time-period** *value*
Parameter Description	**time-period *value***: Indicates the automatic synchronization interval, with the unit of seconds. The value ranges from 1 second to 1 month (2,678,400 seconds).
Command Mode	Redundancy configuration mode
Usage Guide	Configure the automatic synchronization interval of the startup-config and running-config files in the case of redundancy of dual supervisor modules.

Configuration Example

Configuring the Automatic Synchronization Interval

Configuration Steps	In redundancy configuration mode of the master supervisor module, configure the automatic synchronization interval to 60 seconds.
	Hostname(config)# redundancy Hostname(config-red)# auto-sync time-period 60 Redundancy auto-sync time-period: enabled (60 seconds). Hostname(config-red)# exit
Verification	Run the **show redundancy states** command to check the configuration.
	Hostname# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 3600 s

11.5 Monitoring

Displaying

Description	Command
Displays the current redundancy status of dual supervisor modules.	**show redundancy states**

12 Configuring PoE

12.1 Overview

Power over Ethernet (PoE) is a technology that can transmit electricity and data to devices through twisted pairs over Ethernet. This technology enables various devices such as VOIP, WIFI APs, network cameras, hubs and computers to obtain electricity through twisted pairs.

The largest distance that can be powered by a PoE switch is 100 m as defined by the standards. A PoE switch can collect statistics about the power supplies of all ports and the entire device, which can be displayed by a query command.

Protocols and Standards

Currently, PoE complies with the IEEE 802.3af and IEEE 802.3at standards. The following table lists the main characteristics of and differences between the two standards:

Parameter	802.3af	802.3at
Available Power for PD	12.95 W	25.50 W
Maximum Power Provided by PSE	15.4 W	30 W
Voltage Range of PSE	44.0-57.0 V	50.0-57.0 V
Voltage Range of PD	37.0-57.0 V	42.5-57.0 V
Maximum Resistance of Network Cables	20 Ω	12.5 Ω
Power Management Mode	Classify power levels during line initialization.	Classify the power supply into 4 levels during line initialization or dynamically adjust the power supply in the unit of 0.1 W.
Supported Cables	Cat-3 or Cat-5 twisted pairs	Cat-5 twisted pairs

12.2 Applications

Application	Description
PoE Power Supply Scenario	In the scenario, a PoE switch powers powered devices (PDs) and implements data exchange.

12.2.1 PoE Power Supply Scenario

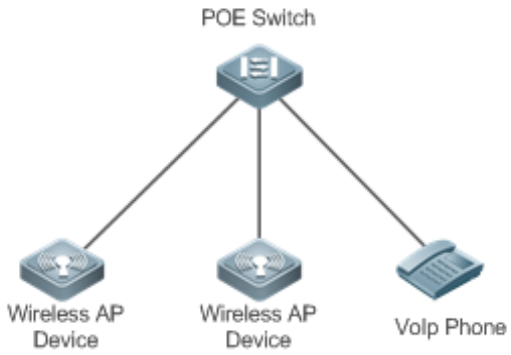
Scenario

In a PoE system set up with a PoE switch, the PoE switch combines the PoE power supply with the PSE. In addition to providing normal network data exchange, the PoE switch also provides the power supply function. The main PDs in the system include the APs of a WLAN and VoIP telephones.

The PoE switch provides power management, including power supply enabling for ports, power supply priority management, over-temperature protection for ports, and power supply status query for devices and ports.

A PoE switch enabling PoE+ supports LLDP correlation with PDs for dynamically managing the power supply power of ports.

Figure 12-1



With constantly increasing functions, terminals consume more and more power. The power consumption of certain terminals exceeds the maximum power 30 W that can be provided by POE+. Consequently, these terminals have to return to the traditional power supply mode.

Deployment

- By default, a PoE switch port is enabled with the power supply function and can start the power supply after detecting an accessed device.
- If the total power of the PoE system is insufficient, you can manually configure the power priority for ports to ensure that the ports are powered first.
- LLDP correlation is enabled by default.

12.3 Features

Basic Concepts

PoE Power Supply

The PoE power supply powers the entire PoE system and is classified into external and internal power supplies. Cassette PoE switches often have internal power supplies and certain products also support external power supplies. External power supplies are called RPS.

PSE

Power Sourcing Equipment (PSE) queries and detects PDs on PoE ports, classifies PDs into different levels, and supplies power for the PDs. After detecting that a PD is removed, the PSE stops supplying power.

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. Switches 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.

Overview

Feature	Description
Power Supply Management for the PoE System	Manages the power supply policies of the system, such as the power supply mode and disconnection detection mode, and supports monitoring on the power supply of the PoE system, such as the system alarm limit and trap sending enabling/disabling.
Power Supply Management for PoE Ports	Manages the power supply policies of PoE ports, such as port enabling and power supply prioritization.
Auxiliary PoE Power Supply Functions	Provides auxiliary power supply management functions for the system, such as the power alarm limit of the system and PD descriptor configuration of ports.

12.3.1 Power Supply Management for the PoE System

Working Principle

Power supply management for the PoE system supports:

You can switch the power supply mode (namely, the method for allocating power for PDs connected to the PoE switch). The PoE switch supports the auto mode, energy-saving mode and static mode for power supply management.

In the auto mode, the system allocates power based on the detected PD classes and types on ports. A PoE switch allocates power for 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. In this mode, even if there is a device of Class3 that consumes only 11 W, the PoE switch allocates a power of 15.4 W for the port connecting to this device. The auto mode is the default power supply management mode of the PoE switch.

In the energy-saving mode, the PoE switch dynamically adjusts allocated power based on actual consumption of PDs. In this mode, the PoE switch can power more PDs, but the power fluctuation of certain PDs may affect the power supply of other PDs. The energy-saving mode is an optional mode of the PoE switch. If the switch does not support this mode, corresponding prompt information will be displayed during configuration.

In the energy-saving mode, the PoE switch calculates the power consumption of the system based on the actual power consumption of the PDs. If certain PDs have a large power fluctuation in this mode, overload may occur on the PoE switch, which causes damage of the PoE device. The PoE switch provides a command for setting the reserved power of the PoE system to ensure that the PoE switch always has "rich" power and that the consumed power will not exceed the limit of the PoE switch.

In the static mode, the switch allocates power to each port as configured. If the power is insufficient, it will be allocated to each port based on port ID from low to high. If the switch does not support this mode, a prompt message will be displayed.

The PoE switch 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 switch. After the hot startup is completed, the system recovers the status saved in the configuration file.

Devices provide PoE-compatible commands to support non-standard PoE devices.

Related Configuration

Configuring the Power Supply Management Mode

By default, the power supply management mode is **energy-saving**.

You can run the **poe mode** { **auto** | **energy-saving** | **static** } command to configure the power supply management mode. Since different power management modes provide different methods for allocating power to PDs, mode switching may affect the PDs that can be powered.

Configuring Reserved Power

By default, the reserved power is 0.

You can run the poe reserve-power *int* command to configure the reserved power. When the system switches to the energy-saving mode, this function takes effect. Configuring Uninterruptible Power Supply During Hot Startup

By default, the system disables the uninterruptible power supply function during hot startup.

You can run the **poe uninterruptible-power** command to enable the uninterruptible power supply function during hot startup. The configuration takes effect after being saved. During hot startup of the system, the PoE system supplies stable power for PDs.

Configuring Compatibility with Non-standard PDs

By default, non-PoE devices are not compatible.

You can run the **poe legacy** command to configure compatibility with non-standard PDs.

12.3.2 Power Supply Management for PoE Ports

Working Principle

Power supply management for the PoE ports supports:

You can enable or disable the PoE function for ports.

You can configure power supply priorities for ports of a PoE switch. The priorities are Critical, High and Low in a descending order. In the auto and energy-saving modes, ports with high priorities are powered first. When the system power of the PoE switch 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 means 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 a switch to manage the power-on/off 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. 10 seconds later, the port is powered on again. 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.

Related Configuration

Enabling the Power Supply Function for a Port

By default, ports are enabled with the PoE power supply function.

You can run the **no poe enable** command to disable the PoE function for ports.

Configuring Power Supply Priorities for Ports

By default, the power supply priorities of ports are low.

You can run the **poe priority** { **low | high | critical** } command to configure the power supply priority of a port. If the power is insufficient, ports with high priorities preempt the power of ports with low priorities. In this case, certain ports with low priorities may be powered off due to insufficient power.

Configuring the Power Allocated to a Port

By default, the power allocated to a port is 0.

You can run the **poe alloc-power** *int* command to configure the power allocated to a port.

Configuring the Maximum Power for Ports

By default, there is no power restriction on ports.

You can run the **poe max-power** *int* command to configure the maximum power for a port. In the static mode, the maximum power configured for a port does not take effect. If the maximum power configured for a port is 15.4 W but the power consumed by the PD connected to the port is greater than 1.1 times of the maximum power, over-current occurs on the port.

Configuring the Regular Power-off Function for a Port

By default, ports do not have the regular power-off function.

You can run the **poe power-off time-range** *range-name* command to configure the regular power-off function for a port. In the clock period specified by **time-range**, the PoE switch does not supply power for connected PDs.

Configuring Compatibility with Non-standard PDs

By default, non-PoE devices are not compatible.

You can run the **poe legacy** command to configure compatibility with non-standard PDs.

Working Principle

The PoE MIB (RFC3621) standard provides **pethMainPseUsageThreshold** to set the power alarm threshold of the system.

PoE switches 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 switches provide the CLI to set this value.

Related Configuration

Configuring the Power Alarm Threshold of the System

By default, the power alarm threshold of the system is 90.

You can run the **poe warning-power** *int* command to configure the power alarm threshold of the system.

Configuring the Trap Notification Sending Switch of the System

By default, the system disables sending of trap notifications.

You can run the **poe notification-control enable** command to enable trap notification sending of the system.

Configuring the PD Descriptor of a Port

By default, a port has no PD descriptor.

You can run the **poe pd-description** *pd-name* command to configure the PD descriptor for the port.

12.4 Configuration

Configuration	Description and Command	
Configuring Power Supply of the PoE System	⚠ (Mandatory) It is used to manage the PoE power supply of the system.	
	poe mode	Configures the power supply management mode.

Configuration	Description and Command	
	poe uninterruptible-power	Configures uninterruptible power supply during hot startup.
	reserve-power	Configures the reserved power.
Configuring Power Supply on PoE Ports	⚠ (Mandatory) It is used to manage the PoE power supply of a specific port.	
	poe enable	Enables the power supply function for a port.
	poe priority	Configures the power supply priority for the port.
	poe max-power	Configures the maximum power allocated to the port.
	poe power-off time-range name	Configures the regular power-off function for the port.
	poe legacy	Configures compatibility with non-standard PDs.
Configuring Auxiliary PoE Power Supply Functions	⚠ (Optional) It facilitates PoE system management.	
	poe warning-power	Configures the power alarm threshold of the system.
	poe notification-control enable	Configures the trap notification sending switch of the system.
	poe pd-description	Configures the PD descriptor of a port.
Enabling the LLDP Classification	⚠ (Optional) It is used to manage the LLDP classification between the PoE and PDs.	
	poe class-lldp enable	Uses the LLDP classification.

12.4.1 Configuring Power Supply of the PoE System

Configuration Effect

- Configure **mode** and change the power allocation mode for PDs. In the auto mode, power is allocated based on PD classes. In the energy-saving mode, power is allocated based on actual consumption. In the static mode, power is allocated based on the **alloc-power** command.
- Configure **reserve-power** to reserved power.
- Configure **uninterruptible-power**, which maintains the PoE power supply function during hot startup.

Configuration Steps

↘ Configuring the Power Supply Management Mode

- (Mandatory) It is energy-saving by default.
- Switch the power supply management mode, power off all PoE ports and then power on them based on the new power supply management mode.

- If the port requires stable power supply, configure the **static** mode. To ensure that the PoE switch powers more ports, you can use the energy-saving mode and allocate power to the ports based on actual power consumption.
- Support the global configuration and port-based configuration.

Configuring the Reserved Power of the System

- (Mandatory) It takes effect only in the energy-saving mode.
- Set the system reserved power command, which takes effect only when the current PoE switch is in the energy-saving mode.
- Setting the reserved power in the energy-saving mode may cause power-off of ports that have been powered on.
- Support the global configuration.

Configuring Uninterruptible Power Supply During Hot Startup

- (Optional) It is disabled by default.
- In actual application, switches may need to be upgraded. For example, after the management software is upgraded, a PoE switch needs to be restarted. However, many PDs are normally powered by the PoE switch 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.
- After this function is enabled or disabled, the configuration will take effect upon next reset only after being saved.
- Support the global configuration.

Verification

View the power supply status of the PoE system to check whether the configuration is correct and whether the configuration takes effect for the power supply.

Related Commands

Configuring the Power Supply Management Mode

Command	**poe mode** { **auto** | **energy-saving** | **static** }
Parameter Description	{ **auto** | **energy-saving** | **static** }: Indicates the auto, energy-saving and static mode.
Command Mode	Global configuration mode
Usage Guide	-

Configuring Reserved Power of System

Command	**poe reserve-power** *int*
Parameter Description	*Int*: Indicates the percentage of the reserved power. <0~50>
Command	Global configuration mode

Mode	
Usage Guide	-

Configuring Uninterruptible Power Supply During Hot Startup

Command	**poe uninterruptible-power**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

Configuring the Power Supply Management Policies for the System

Scenario	● 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.
Configuration Steps	● Switch the mode to the energy-saving mode. ● Sets the reserved power to 20%. ● Support uninterruptible power supply during hot startup.

	`Hostname# configure terminal`
	`Hostname(config)# poe mode energy-saving`
	`Hostname(config)# poe reserve-power 20`
	`Hostname(config)# poe uninterruptible-power`
	`Hostname(config)# exit`
	`Hostname# write`

Verification	Run the **show poe powersupply** command to view the configurations and the power supply information.

	`Hostname#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 : 100.0 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 reserve power : 20 PSE available reserve power : 25.0 W PSE warning power : 90

12.4.2 Configuring Power Supply on PoE Ports

Configuration Effect

- Configure **time-range** to ensure that ports are not powered off within the time-range.
- Configure **priority** for ports. 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 **legacy** to configure compatibility with non-standard PD devices.
- Configure **max-power** for ports. If the power consumed by a port exceeds 1.1 times of the max-power, the power is powered off. After a penalty period of 10 seconds, the port is powered on again.
- Configure **alloc-power** to allocate power in static mode.
- Configure **special** to support PDs with high leakage current.

Configuration Steps

Enabling the Power Supply Function for a Port

- (Mandatory) It is enabled by default.
- To enable or disable the PoE function for a port, you must enable or disable the power supply function of the port.
- By default, the PoE function of the port for connecting a convergence switch is enabled and the PoE function for a core switch is disabled.
- 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 process, which is normal.
- Support port-based configuration.

Configuring the Regular Power-off Function for a Port

- Optional.
- When the power supply function is enabled for a port, configure **time-range** and then manage the power-on/off of the port based on the period of time specified by *range-name*.
- The accuracy of the regular power supply function for a PoE port is one minute and 30 seconds.
- Configure the regular power-off function for a PoE port. **range-name** indicates the name of the time range, consisting of up to 32 characters.
- Support port-based configuration.

Configuring the Power Supply Priority for a Port

- (Mandatory) The priority of a port is low by default.
- In scenarios with insufficient power, in order to supply stable power for certain ports, you can configure priorities for the ports.
- Support the global configuration and port-based configuration.

Configuring Compatibility with Non-standard PDs

- (Optional) It is not supported by default.
- If connected PDs do not meet the PoE standard, the function of being compatible with non-standard PDs can be enabled to supply power for the PDs.
- Running this command for ports not connected to PDs may cause burning of peer devices due to incorrect power-on. Therefore, you must run this command when PDs are connected to ports.
- For standard PoE devices, the class is 4.
- If this command is not configured, non-standard PDs connected will not be powered on and the system will not display any prompt information.

Configuring the Maximum Power Allocated to a Port

- (Optional) There is no maximum power restriction on a port by default.
- This command may take effect in the auto and energy-saving modes.
- When max-power is set to 0, the port is powered off and will not be powered on again.
- Only support 802.3af PoE switch. The max-power ranges from 0 to 15.4.
- Configure the maximum power of a port. The maximum power cannot exceed 1.1 times of the configured power to reduce the impact of high power consumed by a single port on power management.
- Support port-based configuration.

Configuring the Power Allocated to a Port

- (Optional) This command is active only in static mode.
- This command is required static mode.
- If the system power is insufficient when power allocated to a port is configured, the system prompts that the configuration fails.
- When alloc-power is set to 0 in static mode, the port is powered off and will not be powered on again.
- Support port-based configuration.

Configuring Special Power Supply Mode for a Port

- (Optional) By default, the special power supply mode is not supported.
- If a PD with a leakage fault is connected to the port, you can enable the special mode to supply power to the PD.
- If this command is not configured, when a PD with a leakage fault is connected, the PD is not powered on and no prompt is displayed.
- You can configure the specifical power supply mode for a single port.

Verification

View the PoE information of PoE ports to check whether the configuration is correct and whether the configuration takes effect for the power supply.

Related Commands

Enabling the Power Supply Function for a Port

Command	**poe enable**
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Regular Power-off Function for a Port

Command	**poe power-off time-range** *name*
Parameter Description	*name*: Indicates the descriptor of **time-range**.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring Power Supply Priorities for Ports

Command	**poe priority { low | high | critical }**
Parameter Description	{ low | high | critical }: Indicates the priority. The value can be **Low**, **High** or **Critical**.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring Compatibility with Non-standard PDs

Command	**poe legacy**

Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuring the Maximum Power Allocated to a Port

Command	**poe max-power** *int*
Parameter Description	*Int*: Indicates the maximum power, ranging from 0 to 30-95 W. The value ranges from 0 to 15.4 for a system supporting only802.3af.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Power Allocated to a Port

Command	**poe alloc-power int**
Parameter Description	*Int*: Indicates the maximum power, ranging from 0 to 30 W.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

Configuring the Power Supply Management Policies for a Port

Scenario	● The port g0/1 requires a stable power supply not affected by the network environment. ● The power is powered off from 8:00 to 12:00 and is powered on in other time. ● The maximum power of the port does not exceed 17 W.
Configuration Steps	● Set the priority of the port g0/1 to critical. ● Configure **time-range** and associate the port **time-range** configuration of the PoE. ● Set the maximum power of the port g0/1 to 15.4 W.
	Hostname# configure terminal Hostname(config)# time-range poe-time Hostname(config-time-range)# periodic daily 8:00 to 12:00 Hostname(config-time-range)# exit Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if)# poe power-off time-range poe-time

	Hostname(config-if)# poe priority critical Hostname(config-if)# poe max-power 15.4
Verification	Run the **show poe interface gigabitEthernet 0/1** command to view the configurations and the power supply information.
	Hostname#show poe interface gigabitEthernet 0/1 Interface : gi0/1 Power enabled : enable Power status : on Max power : 15.4W Allocate power : N/A 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 Special : off Power-off time-range : poe-time Power management : auto

12.4.3 Configuring Auxiliary PoE Power Supply Functions

Configuration Effect

- Configure **warning-power** to display a warning when the power used by the system exceeds the alarm threshold.
- Configure **notification-control** to control whether the system sends trap notifications in case of power change and port power-on/off.
- Configure **pd-description** to identify the PD connected to a port.

Configuration Steps

Configuring the Power Alarm Threshold of the System

- (Mandatory) It is 99 by default, which is consistent with that specified in the RFC3621 MIB.
- 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.
- Support the global configuration.

Configuring the Trap Notification Sending Switch of the System

- (Mandatory) It is disabled by default.
- When trap notification sending is enabled, trap notifications will be sent when the alarm power notification and power on/off notification of the system are enabled and disabled.
- This CLI command can control only sending of trap notifications defined in the RFC3621 and does not take effect for trap notifications not defined in the RFC3621.
- When sending of trap notifications 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 notification 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 notification will be sent if the alarm power is always lower than the system power subsequently.
- Support the global configuration and port-based configuration.

Configuring the PD Descriptor of a Port

- (Optional) A port has no PD descriptor by default.
- Configure the PD descriptor of a 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.
- Support port-based configuration.

Verification

Check whether alarm information is output when the power used by the system fluctuates on the alarm power threshold to check whether the alarm power configuration takes effect.

Connect the PoE to the SNMP server and power on and off a port to check whether corresponding trap notifications are received from the server and check whether the trap configuration takes effect.

View the PoE information of the port to check whether the PD descriptor of the port is correct.

Related Commands

Configuring the Power Alarm Threshold of the System

Command	**poe warnig-power** *int*
Parameter Description	*Int*: Indicates the alarm power percentage, ranging from 0 to 99.
Command Mode	Global configuration mode
Usage Guide	-

Configuring the Trap Notification Sending Switch of the System

Command	**poe notification-control enable**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuring the PD Descriptor of a Port

Command	**poe pd-description** *pd-name*
Parameter Description	*pd-name*: Indicates the PD descriptor name. The parameter value is a string and supports a maximum of 32 characters.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

Configuring the Power Supply Management Policies for the System

Scenario	● When the 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.
Configuration Steps	● Set the alarm power threshold of the system to 80%. ● Enable the trap notification sending switch of the system. ● Configure the PD descriptor of the port g0/1 as ap220.
	Hostname# configure terminal Hostname(config)# poe poe warnig-power 80 Hostname(config)# poe notification-control enable Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if)# poe pd-description ap220

Verification	Run the **show running-config** command to view the configurations and power supply information.

12.5 Monitoring

Displaying

Description	Command
Displays the PoE configuration and status of a specified port.	**show poe interface**
Displays the PoE status or configurations of all ports.	**show poe interfaces**
Displays the power supply status of the current PoE system.	**show poe powersupply**

13 Configuring Package Management

13.1 Overview

Package management (pkg_mgmt) is a package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying and maintaining various components of the device, among which upgrade is the main function. Through upgrade, users can install new version of software that is more stable or powerful. Adopting a modular structure, the system not only supports overall upgrade and subsystem upgrade but also supports separate upgrade of a feature package.

Component upgrade described in this document applies to both the box-type device and rack-type device. In addition, this document is for only version 11.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

13.2 Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem firmware like boot, kernel, and rootfs on the box-type device and rack-type device.
Upgrading/Degrading a Single Feature Package	Upgrade a single feature package on the box-type device and rack-mount device.
Auto-Sync for Upgrade	Configure the auto sync policy, range and path.

13.2.1 Upgrading/Degrading Subsystem

Scenario

After the upgrade of a subsystem firmware is complete, all system software on the device is updated, and the overall software is enhanced. Generally, the subsystem firmware of the box-type device is called main package.

The main features of this upgrade mode are as follows: All software on the device is updated after the upgrade is completed; all known software bugs are fixed. It takes a long time to finish upgrade.

Deployment

You can store the main package in the root directory of the TFTP server, download the package to the device, and then run an upgrade command to upgrade the package locally. You can also store the main package in a USB flash drive, connect the USB flash drive to the device, and then run an upgrade command to upgrade the package.

13.2.2 Upgrading/Degrading a Single Feature Package

Scenario

Device software consists of several components, and each component is an independent feature module. After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced with the other features unchanged.

The features of this upgrade mode are as follows: Generally, a feature package is small and the upgrade speed is high. After the upgrade is completed, only the corresponding functional module is improved, and other functional modules remain unchanged.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive, connect the USB flash drive to the device, and then complete the upgrade.

13.2.3 Auto-Sync for Upgrade

Scenario

Auto-sync upgrade aims to ensure the coordination of multiple modules (line cards and chassis) within a system on a rack-type device. Specifically, the upgrade firmware is pushed to all target members automatically and the software version of new members is upgraded automatically based on the auto-sync policy.

Deployment

- Configure the policy for auto-sync upgrade.
- Configure the path of firmware for auto-sync upgrade.

13.3 Features

Basic Concepts

Subsystem

A subsystem exists on a device in the form of images. The subsystems of the system include:

- boot: After being powered on, the device loads and runs the boot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.
- kernel: kernel is the OS core part of the system. This subsystem shields hardware composition of the system and provides applications with abstract running environment.
- rootfs: rootfs is the collection of applications in the system.

Main Package and Rack Package

- Main package is often used to upgrade/degrade a subsystem of the box-type device. The main package is a combination package of the boot, kernel, and rootfs subsystems. The main package can be used for overall system upgrade/degradation.

Feature Package of system

- The feature package of system refers to a collection which enables a certain feature. When the device is delivered, all supported functions are contained in the rootfs subsystem. You can upgrade only a specific feature by upgrading a single feature package.

⚠ "Firmware" in this document refers to an installation file that contains a subsystem or feature module.

Overview

Feature	Description
Upgrading/Degrading and Managing Subsystem Components	Upgrades/degrades a subsystem.
Upgrading/Degrading and Managing Functional Components	Upgrades/degrades a functional component.
Auto-Sync for Upgrade	Ensures uniform upgrade upon member change.

13.3.1 Upgrading/Degrading and Managing Subsystem Components

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystem components of the device with the subsystem components in the firmware. The subsystem component contains redundancy design. Subsystems of the device are not directly replaced with the subsystems in the package during upgrade/degradation in most cases. Instead, subsystems are added to the device and then activated during upgrade/degradation.

Working Principle

Upgrade/Degradation

Various subsystems exist on the device in different forms. Therefore, upgrade/degradation varies with different subsystems.

- boot: Generally, this subsystem exists on the norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.
- kernel: This subsystem exists in a specific partition in the form of files. Therefore, upgrading/degrading this subsystem is to write the file.
- rootfs: Generally, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the nandflash device.

Management

Query the subsystem components that are available currently and then load subsystem components as required.

Each subsystem component contains redundancy design. During the upgrade/degradation:

- boot: The boot subsystem always contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is involved in the upgrade, and the slave boot subsystem serves as the redundancy backup all along.
- kernel: as the kernel subsystem contains at least one redundancy backup. More redundancy backups are allowed if there is enough space.
- rootfs: The rootfs subsystem always contains a redundancy backup.

The boot component is not included in the scope of subsystem management due to its particularity. During upgrade of the kernel or rootfs subsystem component, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem component, and management information about various versions.

Relevant Configuration

↘ Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

13.3.2 Upgrading/Degrading and Managing Functional Components

Working Principle

In fact, upgrading a feature is replacing feature files on the device with the feature files in the package.

Managing feature components is aimed at recording the information of feature components by using a database. In fact, installing, displaying and uninstalling a component is the result of performing the Add, Query and Delete operation on the database.

Relevant Configuration

↘ Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

13.3.3 Auto-Sync for Upgrade

Working Principle

Auto-sync upgrade aims to ensure the coordination of multiple modules (line cards and chassis) within a system. Specifically, the upgrade firmware is pushed to all target members automatically and the software version of new members is upgraded automatically based on the auto-sync policy.

There are three policies available.

None: No auto-sync upgrade.

Compatible: Performs auto-synchronization based on the sequential order of versions.

Coordinate: Synchronizes with the version based on the firmware stored on the supervisor module.

Auto-sync is performed in the following scenarios:

If no upgrade target is specified, the firmware is pushed to all matching members(including line cards and chassis) for auto-sync.

Every member is checked when the device is restarted and auto-sync is performed accordingly.

Every new member is checked when added into the system and auto-sync is performed accordingly.

Management

Auto-upgrade policy, range and path should be configured in advance.

Relevant Configuration

Configuring Auto-Sync Policy

To perform upgrade as expected, check the configuration in advance, such as the path.

If some line cards are not checked for upgrade because the system is not configured with auto-sync policy . You can upgrade them manually.

13.4 Configuration

Configuration	Description and Command	
Upgrading/Degrading a Firmware	⚠ The basic function of the configuration is installing and upgrading/degrading a subsystem firmware, and feature package. This command is valid on both the box-type device and rack-type device.	
	upgrade *url* [**force**]	*url* is a local path where the firmware is stored. This command is used to upgrade the firmware stored on the device.
	upgrade download tftp:// *path* [**force**]	*path* is the path of the firmware on the TFTP server. This command is used to download a firmware from the server and upgrade the package automatically.
	upgrade download ftp://*path* [**force**]	*path* is the path of the firmware on the FTP server. This command is used to download a firmware from the server and upgrade the package automatically.
Auto-Sync for Upgrade	(Optional) Configures auto-sync policy.	
	upgrade auto-sync policy [**none** | **compatible** | **coordinate**]	Configures the auto-sync policy.
	upgrade auto-sync range [**chassis**]	Configures the auto-sync range.
	upgrade auto-sync package *url*	Configures the auto-sync path.

13.4.1 Upgrading/Degrading a Firmware

Configuration Effect

Available firmwares include the main package, rack package, and various feature packages packages.

- After the upgrade of the main package is complete, all system software on the line card is updated, and the overall software is enhanced.
- After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced, with other features remain unchanged.

Generally a main package is released to upgrade a box-type device.

Notes

N/A

Configuration Steps

Upgrading the Main Package for a Single Device

- Optional configuration. This configuration is required when all system software on the device needs to be upgraded.
- Download the firmware to the local device and run the **upgrade** command.

Generally a main package is pushed to upgrade a box-type device.

Upgrading Each Feature Package

- Optional configuration. The configuration is used to fix bugs of a certain feature and enhance the function of this feature.

Verification

- After upgrading a subsystem component, you can run the **show upgrade history** command to check whether the upgrade is successful.
- After upgrading a feature component, you can run the **show component** command to check whether the upgrade is successful.

Commands

Upgrade

Command	**upgrade** *url* [**force**]
Parameter Description	**force** indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**upgrade download tftp:/***path* [**force**] **upgrade download oob_tftp:/***path* [**force**]
Parameter Description	**force** indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**upgrade download ftp:/***path* [**force**] **upgrade download oob_ftp:/***path* [**force**]
Parameter Description	*path* indicates the path of installation packages on the ftp server This command is downloaded and upgraded automatically from the server. **force** indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Firmware Stored on the Device

Command	**show upgrade file** *url*
Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Upgrade History

Command	**show upgrade history**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Feature Components Already Installed

Command	**show component**
Parameter Description	[*component_name*]: component name When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component

	works properly.
Command Mode	Privileged EXEC mode
Usage Guide	All parameters are applicable to only the rack-type device.

Configuration Example

Example of Upgrading a Subsystem Firmware on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, insert the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the upgrade command. ● After upgrading the subsystem, restart the device.
Verification	● Check the system version on the current device. If the version information changes, the upgrade is successful.

Example of Upgrading a Feature Package on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive .
Configuration Steps	● Run the **upgrade** command. ● Check whether the device needs to be restarted based on the prompt displayed after the upgrade.
Verification	● Check the version of the feature component on the current device. If the version information changes, the upgrade is successful.

```
Hostname# show component
Package  :sysmonit
    Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2011
    Size:12877    Install time :Wed  Mar 5 14:23:12 2012
    Description:this is a system monit package
    Required packages: None
------------------------------------------------------------------
 package:bridge
    Version: 2.3.1.1252ea       Build time: Wed Dec  7 00:54:56 2011
    Size:26945    Install time : Wed Mar 19:23:15 2012
    Description:this is a bridge package
    Required packages: None
```

Common Errors

If an error occurs during the upgrade, the upgrade module displays an error message. The following provides an example:

```
Upgrade info [ERR]
       Reason:creat config file err(217)
```

The following describes several types of common error messages:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. It is recommended to obtain the firmware again and perform the upgrade operation.
- Firmware not supported by the device: The cause is that you may use the firmware of other devices by mistake. It is recommended to obtain the firmware again, verify the package, and perform the upgrade operation.
- Insufficient device space: Generally, this error occurs on a rack-type device. It is recommended to check whether the device is supplied with a USB flash drive. Generally, this device has a USB flash drive.

13.4.2 Auto-Sync for Upgrade

Configuration Effect

Auto-sync policy, range and path is configured.

Notes

N/A

Configuration Steps

↘ **Configuring Auto-Sync Policy**

Run the **upgrade auto-sync policy command** to configure the auto-sync policy. There are three modes available:

None: No auto-sync upgrade.

Compatible: Performs auto-synchronization based on the sequential order of versions.

Coordinate: Synchronizes with the version based on the firmware stored on the supervisor module.

Configuring Auto-Sync Range

Run the **upgrade auto-sync range** command to configure the auto-sync range. There are two ranges available:

chassis: Performs auto-sync on a chassis.

Configuring Auto-Sync Path

Every time the system is upgraded, the firmware path is recorded automatically for later auto-sync upgrade. Alternatively, use the **upgrade auto-sync package** command to set a path.

Verification

Run the **upgrade auto-sync** command to check the configuration.

Commands

Configuring Auto-Sync Policy

command	**upgrade auto-sync policy** [**none** | **compatible** | **coordinate**]
Parameter Description	**none**: No auto-sync upgrade **compatible**: Performs auto-synchronization based on the sequential order of versions. **coordinate**: Synchronizes with the version based on the firmware stored on the supervisor module.
Command Mode	Privileged EXEX mode
Usage Guide	It is recommended to set **coordinate**.

Configuring Auto-Sync Range

command	**upgrade auto-sync range** [**chassis**]
Parameter Description	**chassis**: Performs auto-sync on a chassis.
Command Mode	Privileged EXEX mode
Usage Guide	N/A

	All parameters are applicable to only the box-type device.

Configuring Auto-Sync Path

command	**upgrade auto-sync package** *url*
Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEX mode
Usage Guide	The path is not set generally. All parameters are applicable to only the rack-type device.

Configuration Example

Configuring Auto-Sync Policy

Configuration Steps	Configure the auto-sync policy.
	`Hostname# upgrade auto-sync policy coordinate` `Upgrade auto-sync policy is set as coordinate`
Verification	Check the auto-sync policy.

Configuring Auto-Sync Range

Configuration Steps	Configure the auto-sync range.
	`Hostname# upgrade auto-sync range chassis` `Upgrade auto-sync range in the range of chassis.`
Verification	Check the auto-sync range.

Common Errors

url is not valid.

13.5 Monitoring

Displaying

Function	Command
Displays all components already installed on the current device and their information.	**show component** [*component_name*]
Displays the upgrade history.	**show upgrade history**

14 SF-APP

14.1 Overview

The overall idea is to integrate the advantages of the Ethernet and PON to make best use of their advantages and avoid their weaknesses so that the products and solutions can better meet customers' requirements. The solution will be iterated in phases. SF-APP is a customized app of the Simplified Optical Ethernet Solution on the device side.

14.2 Features

Features

Feature	Description
Enabling the automatic configuration restore function.	Check whether a specified IPv4 or IPv6 address is reachable and output related information.

14.2.1 Enabling the Automatic Configuration Restore Function

Working Principle

SF-APP notifies and monitors LLDP neighbor advertisements. When the app identifies that the neighbor of the uplink aggregation device is lost (the neighbor information is lost) or the interface connected to the uplink aggregation device is changed (the neighbor information is changed), the customized app actively initiates the configuration restore function. The system clears the existing configuration of the device, re-initiates the online process, and re-obtains the configuration information from the RG-ONC server to recover configuration automatically.

Related Configuration

- Run the **auto-config-recovery** command to configure the function.

14.2.2 Enabling the MIB Node Data Collection Function

Working Principle

In the scenario of a metropolitan area network (MAN) of general education, some functions of simple network management protocol (SNMP) are limited in network address translation (NAT) scenarios. A file is used to send the device information to the ONC server. The system supports obtaining information periodically and in real time. The system obtains the data information of each MIB node through SNMP and saves the data information in a file. After the MIB node information is collected, the file is sent to the ONC server through hyper text transfer protocol (HTTP) in a compressed package.

Related Configuration

Configuring the Interval to Collect MIB Node Information

- The default interval to upload files is 30 min. Run the **auto-collect upload interval** command to configure the interval.

Configuring the Path to Upload MIB Node Information Files to a Server

- No sever path is configured by default. Run the **auto-collect upload url** command to specify a server path.

Enabling the Real-Time MIB Node Data Collection Function

- Run the **auto-collect upload table** command to enable the real-time MIB node data collection function. The data is sent to the ONC server immediately after collected.

14.3 Configuration

Configuration	Description and Command	
Enabling the Automatic Configuration Restore Function	(Optional) It is used to enable the automatic configuration restore function.	
	auto-config-recovery	Enables the automatic configuration restore function.
	(Optional) It is used to specify the interval to collect MIB node information.	
	auto-collect upload interval	Specifies the interval to collect MIB node information.
	(Optional) It is used to specify the interval to collect MIB node information.	
	auto-collect upload url	Specifies the path to upload MIB node information files to a server.
	(Optional) It is used to enable the real-time MIB node data collection function.	
	auto-collect upload table	Enables the real-time MIB node data collection function.

14.3.1 The Automatic Configuration Restore Function

Configuration Effect

After enabling the automatic configuration restore function, in the following two cases, the customized app triggers the device to clear configurations, restart, re-initiate the online process, and re-obtain the configuration information.

Case 1: The neighbor information of uplink aggregation devices is lost.

Case 2: The interface connected to the uplink aggregation device is changed. The device fails to connect to the server within two minutes.

Notes

After the automatic configuration restore function is enabled, the device goes online again, obtains configurations and restarts.

Configuration Steps

- Run the **auto-config-recovery** command to enable the automatic configuration restore function on the device.

Verification

- Enter the **auto-config-recovery** command to display relevant information on the CLI interface.

Related Commands

Ping IPv4

Command	**auto-config-recovery**
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	The automatic configuration restore function is disabled by default. This function is enabled only after running the **auto-config-recovery** command.

Configuration Example

Enabling the Automatic Configuration Restore Function

Configuration Steps	Enable the automatic configuration restore function in the global configuration mode.

	`Hostname#config`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)#auto-config-recovery`
	`Hostname(config)#show run | in auto-config-recovery`
	`auto-config-recovery`
	`Hostname(config)#`

Verification	Run the **show run** command to check whether the **auto-config-recovery** file exists.

14.3.2 The Real-Time MIB Node Data Collection Function

Configuration Effect

In NAT scenarios, the function to directly obtain MIB node information through SNMP is limited and cannot work normally. In this case, the system collects MIB node data, writes the data to files, compress files through HTTP and sends them to the ONC server.

Notes

To trigger the device to collect MIB node information, specify a path to save files to the server first. Otherwise, the system does not collect MIB node information.

Configuration Steps

Configuring the Interval to Collect MIB Node Information Automatically

- Optional. Specify the interval to collect MIB node information. The default interval is 30 minutes.
- Run the **auto-collect upload interval** command in the global configuration mode to specify the interval.

Configuring a Server File Path

- Mandatory. Specify the path to upload compressed files to a server.
- Run the **auto-collect upload url** command in the global configuration mode to specify a server file path.

Collecting MIB Node Data in Real Time

- Collect MIB node data in real time. Collect different MIB node data based on specified parameters. It is not a configuration command.
- Run the **auto-collect upload table** command in the privileged EXEC mode to specify MIB node data to be collected.

Verification

The system collects MIB node information, writes data to files and sends data to the ONC server through HTTP.

Related Commands

Configuring the Interval to Collect MIB Node Information Automatically

Command	**auto-collect upload interval** *time*
Parameter Description	The interval to automatically collect MIB node information in seconds. The value range is from 30 to 172800, that is, from 30 seconds to 2 days.
Command Mode	Global configuration mode.
Usage Guide	By default, the system collects MIB node information every 1800 seconds and sends compressed files to SF-APP. You can set different time intervals as needed. Run the **no** or **default** form of this command to restore the default setting.

Configuring the Server File Path

Command	**auto-collect upload url** *url*
Parameter Description	The path to upload files to the server.
Command Mode	Global configuration mode.
Usage Guide	Without a specified path to upload files to the server, the system does not collect MIB node data. You can delete server file paths to save system resources when data collection is not required.

Collecting MIB Node Data in Real Time

Command	**auto-collect upload table** {**arp-table** | **interface-table** | **mac-table** | **system-information** | **all**}
Parameter Description	Specify MIB node data to be collected.
Command Mode	Privileged EXEC mode.
Usage Guide	Configure the corresponding command to enable the function to collect specified MIB node information. The command only collects the information of MIB nodes listed in a metropolitan area network (MAN) for general education. The unlisted MIB nodes are not in the collection range of this command. Specifies different parameters to trigger information collection. Ensure that the server path is specified on the device before running this command to collect information. Because this is not a configuration command, you cannot run the **show run** command to display its configuration.

Configuration Example

Configuring the Interval to Collect MIB Node Information Automatically

Configuration Steps	● Configure the interval to collect MIB node information automatically in the global configuration mode.

	`Hostname#config`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)#auto-collect upload interval 300`
	`Hostname(config)#show run | in auto-collect`
	`auto-collect upload interval 300`
	`Hostname(config)#`

Verification	Run the **show run** command to check whether the **auto-collect upload interval 300** configuration exists.

Configuring a Server Path

Configuration Steps	● Configure a server path in the global configuration mode.

	`Hostname#config`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# auto-collect upload url http://172.30.33.97/vm_share/`
	`Hostname(config)#show run | in auto-collect`
	`auto-collect upload url http://172.30.33.97/vm_share/`
	`Hostname(config)#`

Verification	Run the **show run** command to check whether the **auto-collect upload url http://172.30.33.97/vm_share/** configuration exists.

Configuration Example

Configuring the Interval to Collect MIB Node Information Automatically

Configuration Steps	● Configure the interval to collect MIB node information automatically in the global configuration mode.
	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#auto-collect upload interval 300 Hostname(config)#show run | in auto-collect auto-collect upload interval 300 Hostname(config)#
Verification	Run the **show run** command to check whether the **auto-collect upload interval 300** configuration exists.

Configuring a Server Path

Configuration Steps	● Enable SF-APP to collect MIB node information of MAC address tables in real time in the privileged EXEC mode.
	Hostname# auto-collect upload table mac-table Hostname#
Verification	SF-APP has collected corresponding MIB node information and sent packages to the specified server path.

15 Configuring Hotkeys

15.1 Overview

Hotkeys are used to maintain and debug devices, including obtaining debugging information.

When a device malfunctions or cannot be controlled properly, you can use hotkeys to check memory information, interrupt information, lock occupancy status, and process information of the device. In addition, you can restart the device, perform one-click collection, and enable/disable the logging function of the console. You can use hotkeys to obtain crucial debugging information of the device to locate the cause of the device exception and restore the device.

15.2 Applications

Application	Description
Displaying Memory Information	Use hotkeys to obtain memory statistics of the device.
Performing One-Click Collection	Perform one-click collection to collect running information of the device.

15.2.1 Displaying Memory Information

Scenario

If you fail to collect memory information of the device through the CLI when an exception occurs during device running, you can use hotkeys on the serial console to collect memory statistics of the device.

Deployment

- Use hotkeys only on the serial console to obtain memory information.

15.2.2 Performing One-Click Collection

Scenario

If an exception occurs during device running and you fail to perform one-click collection through the CLI, you can use hotkeys on the serial console to collect information.

Deployment

- Use hotkeys only on the serial console to perform one-click collection.

15.3 Features

Basic Concepts

Hot Key

Hotkeys, also called magic keys, are used to enter information into the device to obtain debugging information or perform operations on the device to restore device services when the device malfunctions. Supported hotkeys include the **4Esc** key (press the **Esc** key for four consecutive times) or **4$** key (press the **$** key for four consecutive times).

⚠ Hotkeys are available only on the serial console of the device.

4Esc

The **4Esc** key is supported by the device and can implement the following functions:

- Restart the device.
- Enable/Disable the console output.
- Display information about the occupancy of all locks.
- Perform one-click collection.
- Display help information of hotkeys.
- Display CLI debugging information.
- Display interrupt information.

- Display information about processes that have been started.
- Display memory statistics of the device.
- Enable the function of periodically outputting interrupt information.
- Disable the function of periodically outputting interrupt information.
- Disable the log output of the console.
- Display the context switching count and runtime of all threads.
- Display the current stack information of all CPU cores.
- Display the status of all threads.
- Display kernel stack information of all threads.
- Start the task of outputting dots by the console.
- Stop the task of outputting dots by the console.

The **4Esc** key can also be replaced with the **4@** key (press the @ key for four consecutive times).

Overview

Feature	Description
Restarting the device	Restarts the device to restore the device services. For details, see the **4Esc + b** command in *Hotkey Commands*. This function may cause the restart of a device that is running properly. Therefore, save data in advance and use this function only when debugging a device.
Enabling/Disabling the console output	Manages the console output. For details, see the **4Esc + c** command in *Hotkey Commands*.
Displaying information about the occupancy of all locks	Displays debugging information about locks. For details, see the **4Esc + d** command in *Hotkey Commands*.
Performing one-click collection	Performs one-click collection when the console is unavailable. For details, see the **4Esc + f** command in *Hotkey Commands*.
Displaying help information of hotkeys	Displays help information of the **4Esc** hotkeys. For details, see the **4Esc + h** command in *Hotkey Commands*.
Displaying CLI debugging information	Displays CLI debugging information. For details, see the **4Esc + i** command in *Hotkey Commands*.
Displaying interrupt information	Displays interrupt information. For details, see the **4Esc + j** command in *Hotkey Commands*.
Displaying information about started processes	Displays information about started processes. For details, see the **4Esc + l** command in *Hotkey Commands*.
Displaying memory statistics of the device	Displays memory statistics of the device. For details, see the **4Esc + m** command in *Hotkey Commands*.

Enabling the function of periodically outputting interrupt information	Enables the function of periodically outputting interrupt information. For details, see the **4Esc + n** command in *Hotkey Commands*.
Disabling the function of periodically outputting interrupt information	Disables the function of periodically outputting interrupt information. For details, see the **4Esc + o** command in *Hotkey Commands*.
Disabling the log output of the console	Disables the log output of the console. For details, see the **4Esc + p** command in *Hotkey Commands*.
Displaying the context switching count and runtime of all threads	Displays the context switching count and runtime of all threads. For details, see the **4Esc + q** command in *Hotkey Commands*.
Displaying current stack information of all CPU cores	Displays current stack information of all CPU cores. For details, see the **4Esc + r** command in *Hotkey Commands*.
Displaying the status of all threads	Displays the status of all threads. For details, see the **4Esc + s** command in *Hotkey Commands*.
Displaying kernel stack information of all threads	Displays kernel stack information of all threads. For details, see **4Esc + t** command in *Hotkey Commands*.
Starting the task of outputting dots by the console	Starts the task of outputting dots by the console. For details, see **4Esc + x** command in *Hotkey Commands*.
Stopping the task of outputting dots by the console	Stops the task of outputting dots by the console. For details, see **4Esc + y** command in *Hotkey Commands*.

15.4 Configuration

Each function command of the hotkeys is simple and does not rely on other commands. For details about hotkey commands, see *Hotkey Commands*.

15.5 Monitoring

Hotkeys are used for debugging and maintenance of the device. They do not provide other monitoring or maintenance functions.

Ethernet Switching Configuration

1. Configuring Interfaces
2. Configuring MAC Addresses
3. Configuring Aggregated Port
4. Configuring VLAN
5. Configuring Voice VLAN
6. Configuring MSTP
7. Configuring LLDP
8. Configuring QinQ
9. Configuring ERPS

1 Configuring Interfaces

1.1 Overview

Interfaces are important in implementing data switching on network devices. 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 is not a hardware port on the device. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical port or independent of any physical port. For network protocols, physical ports and logical interfaces serve the same function.

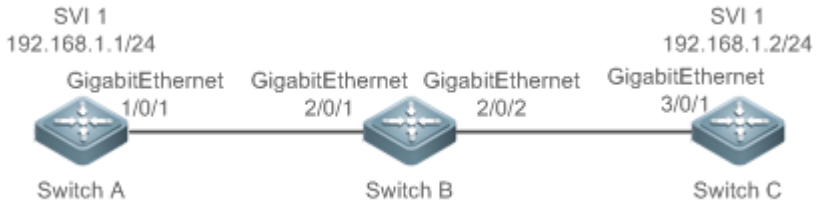
1.2 Applications

Application	Description
L2 Data Switching Through the Physical Ethernet Interface	Implement Layer-2 (L2) data communication of network devices through the physical L2 Ethernet interface.
L3 Routing Through the Physical Ethernet Interface	Implement Layer-3 (L3) data communication of network devices through the physical L3 Ethernet interface.

1.2.1 L2 Data Switching Through the Physical Ethernet Interface

Scenario

Figure 1-1



As shown in Figure 1-1, Switch A, Switch B, and Switch C form a simple L2 data switching network.

Deployment

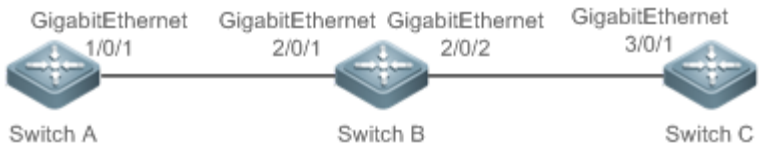
- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthemet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as Trunk ports.

- Create a switch virtual interface (SVI), SVI 1, on Switch A and Switch C respectively, and configure IP addresses from a network segment for the two SVIs. The IP address of SVI 1 on Switch A is 192.168.1.1/24, and the IP address of SVI 1 on Switch C is 192.168.1.2/24.
- Run the **ping 192.168.1.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement data switching through Switch B.

1.2.2 L3 Routing Through the Physical Ethernet Interface

Scenario

Figure 1-2



As shown in Figure 1-2, Switch A, Switch B, and Switch C form a simple L3 data communication network.

Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as L3 routed ports.
- Configure IP addresses from a network segment for GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1. The IP address of GigabitEthernet 1/0/1 is 192.168.1.1/24, and the IP address of GigabitEthernet 2/0/1 is 192.168.1.2/24.
- Configure IP addresses from a network segment for GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1. The IP address of GigabitEthernet 2/0/2 is 192.168.2.1/24, and the IP address of GigabitEthernet 3/0/1 is 192.168.2.2/24.
- Configure a static route entry on Switch C so that Switch C can directly access the network segment 192.168.1.0/24. Configure a static route entry on Switch A so that Switch C can directly access the network segment 192.168.2.0/24.
- Run the **ping 192.168.2.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement L3 routing through Switch B.

1.3 Features

Basic Concepts

↘ Interface Classification

Interfaces on devices fall into two categories:

- L2 interface (Switch)

- L3 interface (supported by L3 devices)

1. Common L2 interfaces are classified into the following types:

- Switch port
- L2 aggregate port (AP)

2. Common L3 interfaces are classified into the following types:

- Routed port
- L3 AP port
- SVI
- Loopback interface

Switch Port

A switch port is an individual physical port on the device, and implements only the L2 switching function. The switch port is used to manage physical ports and L2 protocols related to physical ports.

L2 AP Port

An AP port is formed by aggregating multiple physical ports. Multiple physical links can be bound together to form a simple logical link. This logical link is called an AP port.

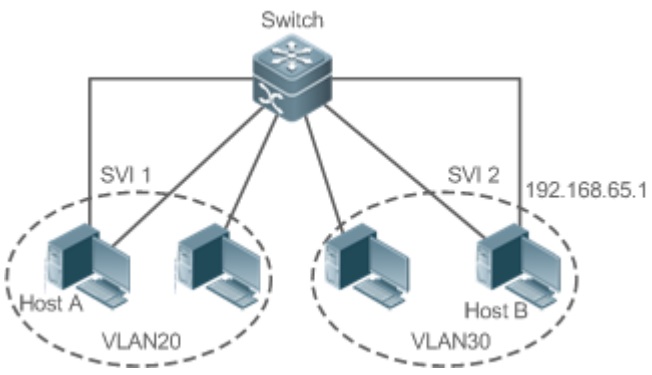
For L2 switching, an AP port is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP port are balanced among the L2 AP member ports. If one member link fails, the L2 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

SVI

The SVI can be used as the management interface of the local device, through which the administrator can manage the device. You can also create an SVI as a gateway interface, which is mapped to the virtual interface of each VLAN to implement routing across VLANs among L3 devices. You can run the **interface vlan** command to create an SVI and assign an IP address to this interface to set up a route between VLANs.

As shown in Figure 1-3, hosts in VLAN 20 can directly communicate with each other without participation of L3 devices. If Host A in VLAN 20 wants to communicate with Host B in VLAN 30, SVI 1 of VLAN 20 and SVI 2 of VLAN 30 must be used.

Figure 1-3



Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. A routed port is not related with a specific VLAN. Instead, it is just an access port. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that you must delete all L2 features of a switch port before running the **no switchport** command.

If a port is a L2 AP member port or a DOT1X port that is not authenticated, you cannot run the **switchport** or **no switchport** command to configure the switch port or routed port.

L3 AP Port

Like the L2 AP port, a L3 AP port is a logical port that aggregates multiple physical member ports. The aggregated ports must be the L3 ports of the same type. The AP port functions as a gateway interface for L3 switching. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP port are balanced among the L3 AP member ports. If one member link fails, the L3 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

A L3 AP port cannot be used for L2 switching. You can run the **no switchport** command to change a L2 AP port that does not contain any member port into a L3 AP port, add multiple routed ports to this L3 AP port, and then assign an IP address to this L3 AP port to set up a route.

Loopback Interface

The loopback interface is a local L3 logical interface simulated by the software that is always UP. Packets sent to the loopback interface are processed on the device locally, including the route information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) routing protocol, or as the source address used by Border Gateway Protocol (BGP) to set up a TCP connection. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface, and you can treat the loopback interface as a virtual Ethernet interface.

Overview

Feature	Description
Interface Configuration Commands	You can configure interface-related attributes in interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created.
Interface Description and Administrative Status	You can configure a name for an interface to identify the interface and help you remember the functions of the interface. You can also configure the administrative status of the interface.
MTU	You can configure the maximum transmission unit (MTU) of a port to limit the length of a frame that can be received or sent over this port.
Bandwidth	You can configure the bandwidth of an interface.
Load Interval	You can specify the interval for load calculation of an interface.
Carrier Delay	You can configure the carrier delay of an interface to adjust the delay after which the status of an interface changes from Down to Up or from Up to Down.
Link Trap Policy	You can enable or disable the link trap function on an interface.

Feature	Description
Interface Index Persistence	You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.
Routed Port	You can configure a physical port on a L3 device as a routed port, which functions as the gateway interface for L3 switching.
L3 AP Port	You can configure an AP port on a L3 device as a L3 AP port, which functions as the gateway interface for L3 switching.
Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode	You can configure the speed, duplex mode, flow control mode, and auto negotiation mode of an interface.
Automatic Module Detection	If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.
Protected Port	You can configure some ports as protected ports to disable communication between these ports. You can also disable routing between protected ports.
Port Errdisable Recovery	After a port is shut down due to a violation, you can run the **errdisable recovery** command in global configuration mode to recover all the ports in errdisable state and enable these ports.
Optical Module Antifake Detection	You can configure the optical module antifake detection function to check whether the optical module in use is supplied bythe vendor.
EEE	You can configure the Energy Efficient Ethernet (EEE) function to enable the interface to work in low power consumption mode.
Port Flapping Protection	You can configure the port flapping protection function so that the system can automatically shut down a port when flapping occurs on the port.

1.3.1 Interface Configuration Commands

You can run the interface command in global configuration mode to enter interface configuration mode. You can configure interface-related attributes in interface configuration mode.

Working Principle

Run the interface command in global configuration mode to enter interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created. You can also run the interface range or interface range macro command in global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same features.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

↘ **Interface Numbering Rules**

In stand-alone mode, the ID of a physical port consists of two parts: slot ID and port ID on the slot. For example, if the slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 2/3. In stack mode, the ID of a physical port consists of three parts: device ID, slot ID, and port ID on the slot. For example, if the device ID is 1, slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 1/2/3.

The device ID ranges from 1 to the maximum number of supported member devices.

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 slot are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of a port on the slot ranges from 1 to the number of ports on the slot, and is numbered sequentially from left to right.

The ID of an AP port ranges from 1 to the number of AP ports supported by the device.

The ID of an SVI is the VID of the VLAN corresponding to this SVI.

Configuring Interfaces Within a Range

You can run the **interface range** command in global configuration mode to configure multiple interfaces at a time. Attributes configured in interface configuration mode apply to all these interfaces.

The **interface range** command can be used to specify several interface ranges.

The **macro** parameter is used to configure the macro corresponding to a range. For details, see "Configuring Macros of Interface Ranges."

Ranges can be separated by commas (,).

The types of interfaces within all ranges specified in a command must be the same.

Pay attention to the format of the **range** parameter when you run the **interface range** command.

The following interface range formats are valid:

- **FastEthernet** device/slot/{first port} - {last port};
- **GigabitEthernet** device/slot/{first port} - {last port};
- **TenGigabitEthernet** device/slot/{first port} - {last port};
- **FortyGigabitEthernet** device/slot/{first port} - {last port};
- **AggregatePort** *Aggregate-port ID* (The AP ID ranges from 1 to the maximum number of AP ports supported by the device.)
- **vlan** vlan-ID-vlan-ID (The VLAN ID ranges from 1 to 4,094.)
- **Loopback** loopback-ID (The loopback ID ranges from 1 to 2,147,483,647.)

Interfaces in an interface range must be of the same type, namely, FastEthernet, GigabitEthernet, AggregatePort, or SVI.

Configuring Macros of Interface Ranges

You can define some macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, you must first run the **define interface-range** command in global configuration mode to define these macros.

Run the **no define interface-range macro_name** command in global configuration mode to delete the configured macros.

1.3.2 Interface Description and Administrative Status

You can configure a name for an interface to identify the interface and help you remember the functions of the interface.

You can enter interface configuration mode to enable or disable an interface.

Working Principle

Interface Description

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

Interface Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

1.3.3 MTU

You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.

Working Principle

When a large amount of data is exchanged over a port, frames greater than the standard Ethernet frame may exist. This type of frame is called jumbo frame. The MTU is the length of the valid data segment in a frame. It does not include the Ethernet encapsulation overhead.

If a port receives or sends a frame with a length greater than the MTU, this frame will be discarded.

1.3.4 Bandwidth

Working Principle

The **bandwidth** command can be configured so that some routing protocols (for example, OSPF) can calculate the route metric and the Resource Reservation Protocol (RSVP) can calculate the reserved bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of the physical port.

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

1.3.5 Load Interval

Working Principle

You can run the **load-interval** command to specify the interval for load calculation of an interface. Generally, the interval is 10s.

1.3.6 Carrier Delay

Working Principle

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from Down to Up or from Up to Down. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If this parameter is set to a great value, nearly every DCD change is not detected. On the contrary, if the parameter is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, the carrier delay should be set to a smaller value to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, the carrier delay should be set to a greater value to avoid topology or route flapping.

1.3.7 Link Trap Policy

You can enable or disable the link trap function on an interface.

Working Principle

When the link trap function on an interface is enabled, the Simple Network Management Protocol (SNMP) sends link traps when the link status changes on the interface.

1.3.8 Interface Index Persistence

Like the interface name, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

Working Principle

After interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.3.9 Routed Port

Working Principle

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that you must delete all L2 features of a switch port before running the **no switchport** command.

1.3.10 L3 AP Port

Working Principle

Like a L3 routed port, you can run the **no switchport** command to change a L2 AP port into a L3 AP port on a L3 device, and then assign an IP address to this AP port to set up a route. Note that you must delete all L2 features of the AP port before running the **no switchport** command.

A L2 AP port with one or more member ports cannot be configured as a L3 AP port. Similarly, a L3 AP port with one or more member ports cannot be changed to a L2 AP port.

1.3.11 Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode

You can configure the interface speed, duplex mode, flow control mode, and auto negotiation mode of an Ethernet physical port or AP port**.**

Working Principle

Speed

Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port.

When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Duplex Mode

- The duplex mode of an Ethernet physical port or AP port can be configured as follows:
- Set the duplex mode of the interface to full-duplex so that the interface can receive packets while sending packets.
- Set the duplex mode of the interface to half-duplex so that the interface can receive or send packets at a time.
- Set the duplex mode of the interface to auto-negotiation so that the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.
- When you configure the duplex mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Flow Control

Two flow control modes are defined for an interface:

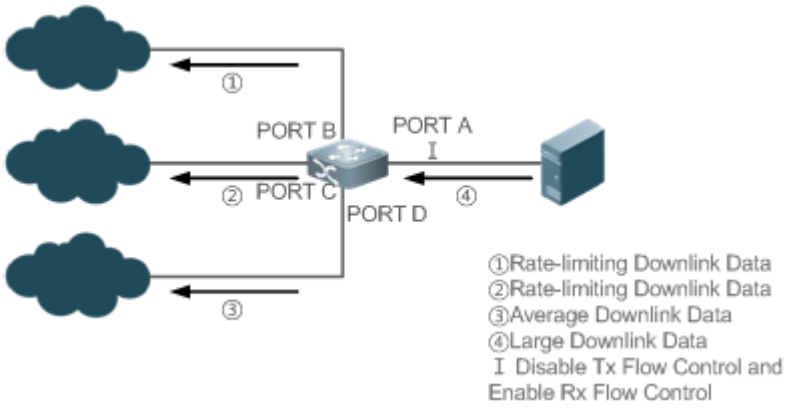
- Symmetric flow control mode: Generally, after flow control is enabled on an interface, the interface processes the received flow control frames, and sends the flow control frames when congestion occurs on the interface. The received and sent flow control frames are processed in the same way. This is called symmetric flow control mode.
- Asymmetric flow control mode: In some cases, an interface on a device is expected to process the received flow control frames to ensure that no packet is discarded due to congestion, and not to send the flow control frames to avoid

decreasing the network speed. In this case, you need to configure asymmetric flow control mode to separate the procedure for receiving flow control frames from the procedure for sending flow control frames.

- When you configure the flow control mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

As shown in Figure 1-4, Port A of the device is an uplink port, and Ports B, C and D are downlink ports. Assume that Port A is enabled with the functions of sending and receiving flow control frames. Port B and Port C are connected to different slow networks. If a large amount of data is sent on Port B and Port C, Port B and Port C will be congested, and consequently congestion occurs in the inbound direction of Port A. Therefore, Port A sends flow control frames. When the uplink device responds to the flow control frames, it reduces the data flow sent to Port A, which indirectly slows down the network speed on Port D. At this time, you can disable the function of sending flow control frames on Port A to ensure the bandwidth usage of the entire network.

Figure 1-4



Auto Negotiation Mode

The auto negotiation mode of an interface can be On or Off. The auto negotiation state of an interface is not completely equivalent to the auto negotiation mode. The auto negotiation state of an interface is jointly determined by the interface speed, duplex mode, flow control mode, and auto negotiation mode.

When you configure the auto negotiation mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

- Generally, if one of the interface speed, 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 speed, duplex mode, and flow control mode is set to auto, and the auto negotiation mode of an interface is Off, the auto negotiation state of the interface is Off, that is, the auto negotiation function of the interface is disabled.
- For a 100M fiber port, the auto negotiation function is always disabled, that is, the auto negotiation state of a 100M fiber port is always Off. For a Gigabit copper port, the auto negotiation function is always enabled, that is, the auto negotiation state of a Gigabit copper port is always On.

1.3.12 Automatic Module Detection

If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.

Working Principle

Currently, the automatic module detection function can be used to detect only the SFP and SFP+ modules. The SFP is a Gigabit module, whereas SFP+ is a 10 Gigabit module. If the inserted module is SFP, the interface works in Gigabit mode. If the inserted module is SFP+, the interface works in 10 Gigabit mode.

The automatic module detection function takes effect only when the interface speed is set to auto.

1.3.13 Protected Port

In some application environments, it is required that communication be disabled between some ports. For this purpose, you can configure some ports as protected ports. You can also disable routing between protected ports.

Working Principle

Protected Port

After ports are configured as protected ports, protected ports cannot communicate with each other, but can communicate with non-protected ports.

Protected ports work in either of the two modes. In the first mode, L2 switching is blocked but routing is allowed between protected ports. In the second mode, both L2 switching and routing are blocked between protected ports. If a protected port supports both modes, the first mode is used by default.

When two protected port are configured as a pair of mirroring ports, frames sent or received by the source port can be mirrored to the destination port.

Currently, only an Ethernet physical port or AP port can be configured as a protected port. When an AP port is configured as a protected port, all of its member ports are configured as protected ports.

Blocking L3 Routing Between Protected Ports

By default, L3 routing between protected ports is not blocked. In this case, you can run the **protected-ports route-deny** command to block routing between protected ports.

1.3.14 Port Errdisable Recovery

Some protocols support the port errdisable recovery function to ensure security and stability of the network. For example, in the port security protocol, when you enable port security and configure the maximum number of security addresses on the port, a port violation event is generated if the number of addresses learned on this port exceeds the maximum number of security addresses. Other protocols, such as the Spanning Tree Protocol (STP), DOT1X, and REUP, support the similar functions, and a violating port will be automatically shut down to ensure security.

Working Principle

After a port is shut down due to a violation, you can run the **errdisable recovery** command in global configuration mode to recovery 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.

1.3.15 Optical Module Alarm Detection

After this function is enabled, you can view the alarm information of the optical module installed in the interface through the MIB tool. When an event such as optical module plugging/exception/exception recovery is detected, related alarm TRAP will be sent to the system. Abnormal events include high and low optical TX power, high and low RX power, IIC failure in the module, and supported module types.

Working Principle

After the alarm detection function is enabled and the detection interval is set, the device will periodically monitor the status of the optical module installed in the interface. When an event is detected, the device will send an alarm TRAP. An optical module plugging event will be notified immediately, while an optical module exception or exception recovery event will be notified within a cycle. Repeated exceptions will only be notified once. Exception events will be notified periodically, and exception recovery events will be notified once. You can disable the periodic notification function by running the repeat notification mode switch command.

1.3.16 Optical Module Antifake Detection

You can configure the optical module antifake detection function to check whether the optical module in use is supplied by the vendor.

If the optical module is not supplied by the vendor, the data communication may be affected. If the optical module antifake detection function is enabled, the device can automatically identify an optical module that is not supplied by the vendor and generate an alarm when such module is installed into the device.

This function is disabled by default. You can enable this function through configuration.

Working Principle

Each optical module supplied by the vendor has a unique antifake code. The device can read this antifake code to determine whether the module is supplied by the vendor. If not, the device will generate syslogs and sends traps.

1.3.17 EEE

Energy Efficient Ethernet (EEE) is an energy efficient Ethernet solution. When EEE is enabled, the port enters low power consumption mode when the Ethernet connection is idle, thus saving the energy.

Low Power Idle (LPI) is the low power consumption mode. After a port enters LPI mode, it reduces signals significantly, and only sends signals that are sufficient to maintain the connection on the port to save the energy.

Working Principle

According to the Ethernet standards or specifications, interfaces with a bandwidth of 100M or above have the 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 to enter LPI mode for the purpose of saving energy. In LPI mode, the power consumption is low when the link is idle. The EEE technology can also quickly change the LPI state of a port to the normal state, providing high-performance data transmission.

After enabled with EEE, the port automatically enters LPI mode if the port is always Up without sending or receiving any packet in a period of time. The port recovers the working mode when it needs to send or receive packets, thus saving the energy. To make the EEE function take effect, the peer port must also support the EEE function.

Only a copper port working in 100M or 1000M speed mode supports the EEE function.

The EEE function takes effect only on the port enabled with auto negotiation.

1.3.18 Port Flapping Protection

When flapping occurs on a port, a lot of hardware interruptions occur, consuming a lot of CPU resources. On the other hand, frequent port flapping damages the port. You can configure the flapping protection function to protect ports.

Working Principle

By default, the port flapping protection function is enabled. You can disable this function as required. When flapping occurs on a port, the port is detected for flapping every 2s or 10s. If flapping occurs 6 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 disabled. If flapping occurs 10 times within 10s on a port, the device displays a prompt without disabling the port.

1.3.19 Syslog

You can enable or disable the syslog function to determine whether to display information about the interface changes or exceptions.

Working Principle

You can enable or disable the syslog function as required. By default, this function is enabled. When an interface becomes abnormal, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

1.3.20 Global MTU

Users can set the global MTU to control the maximum length of frames that can be sent and received over all ports.

Working Principle

When large-throughput data exchange is performed over a port, frames whose length is longer than that of a standard Ethernet frame may exist, and these frames are called jumbo frames. The MTU indicates the length of valid data fields in a frame, excluding the Ethernet encapsulation overhead.

If the length of a frame received or forwarded by a port exceeds the MTU value, the frame will be discarded.

The MTU value ranges from 64 to 9216 bytes. The granularity is four bytes. The default value is 1500 bytes.

- The IP MTU automatically changes to the value of the link MTU of an interface when the globally set link MTU changes.
- The MTU of an interface takes precedence over the global MTU. After the global MTU is configured, the MTU of an interface cannot be set to the default value.

1.3.21 Physical Port Flapping Protection

When flapping occurs on a physical 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.

Working Principle

By default, the phyiscal port flapping protection function is enabled. You can disable this function as required. When flapping occurs on a port, the port is detected for flapping every 30s. If a port flaps 60 times within 30s, one effective flap is considered to have occurred. If three consecutive effective flaps (that is, the physical port is detected continuously within 90 seconds) are detected, the conditions for triggering port violation are met, the port must be shutdown, and the device displays a prompt. If the this function is disabled, the device will also displays a prompt if the conditions for three consecutive effective flaps are met, but the port will not be shudtown because of violation.

1.3.22 Port Auto Down

APD (auto power down) is a way to save energy. If this function is enabled, when a port is not connected, the port enters the power down mode to save energy.

Working Principle

Even when a port is not connected to an Ethernet cable, it will still be in the power supply state, which consumes a large amount of power. When the APD mode is enabled, the device will automatically listen on the signal of the link. If there is no signal on the link (that is, when the Ethernet cable is not inserted), the port will automatically enter the power down mode. When power is detected on the link (that is, when the Ethernet cable is inserted), the port will resume normal operation.

1.4 Configuration

Configuration	Description and Command	
Performing Basic Configurations	(Optional) It is used to manage interface configurations, for example, creating/deleting an interface, or configuring the interface description.	
	interface	Creates an interface and enters configuration mode of the created interface or a specified interface.
	interface range	Enters an interface range, creates these interfaces (if not created), and enters interface configuration mode.
	define interface-range	Creates a macro to specify an interface range.

Configuration	Description and Command	
	snmp-server if-index persist	Enables the interface index persistence function so that the interface index remains unchanged after the device is restarted.
	description	Configures the interface description of up to 80 characters in interface configuration mode.
	snmp trap link-status	Configures whether to send the link traps of the interface.
	shutdown	Shuts down an interface in interface configuration mode.
	physical-port dither protect	Configures the port flapping protection function in global configuration mode.
	logging [link-updown | error-frame | link-dither]	Configures the syslog function on an interface in global configuration mode.
	port-dither protect	Enables port oscillation protection globally.
Configuring Interface Attributes	(Optional) It is used to configure interface attributes.	
	bandwidth	Configures the bandwidth of an interface in interface configuration mode.
	carrier-delay	Configures the carrier delay of an interface in interface configuration mode.
	load-interval	Configures the interval for load calculation of an interface.
	duplex	Configures the duplex mode of an interface.
	flowcontrol	Enables or disables flow control of an interface.
	mtu	Configures the MTU of an interface.
	negotiation mode	Configures the auto negotiation mode of an interface.
	speed	Configures the speed of an interface.
	switchport	Configures an interface as a L2 interface in interface configuration mode. (Run the **no switchport** command to configure an interface as a L3 interface.)
	switchport protected	Configures a port as a protected port.
	protected-ports route-deny	Blocks L3 routing between protected ports in global configuration mode.
	errdisable recovery	Recovers a port in errdisable state in global configuration mode.
	fiber alarm-detect enable	Configures optical module alarm detection function in global configuration mode.
	fiber alarm-detect period	Configures optical module exception event alarm detection interval in global configuration mode.
	fiber alarm-detect repeat-mode	Configures optical module alarm periodic notification function in global configuration mode.

Configuration	Description and Command	
	fiber antifake ignore	Disables the optical module antifake detection function in global configuration mode.
	fiber antifake enable	Enables the optical module antifake detection function in global configuration mode.

1.4.1 Performing Basic Configurations

Configuration Effect

- Create a specified logical interface and enter configuration mode of this interface, or enter configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter interface configuration mode, or enter configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.
- Configure the interface description so that users can directly learn information about the interface.
- Enable or disable the link trap function of an interface.
- Enable or disable an interface.
- Enable or disable port flapping protection.

Notes

- The **no** form of the command can be used to delete a specified logical interface or logical interfaces in a specified range, but cannot be used to delete a physical port or physical ports in a specified range.
- The **default** form of the command can be used in interface configuration mode to restore default settings of a specified physical or logical interface, or interfaces in a specified range.

Configuration Steps

↘ Configuring a Specified Interface

- Optional.
- Run this command to create a logical interface or enter configuration mode of a physical port or an existing logical interface.

Command	**interface** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. The interface can be an Ethernet physical port, AP port, SVI, or loopback interface.
Defaults	N/A
Command	Global configuration mode

Mode	
Usage Guide	● If a logical interface is not created yet, run this command to create this interface and enter configuration mode of this interface. ● For a physical port or an existing logical interface, run this command to enter configuration mode of this interface. ● Use the **no** form of the command to delete a specified logical interface. ● Use the **default** form of the command to restore default settings of the interface in interface configuration mode.

Configuring Interfaces Within a Range

- Optional.
- Run this command to create multiple logical interfaces or enter configuration mode of multiple physical port or existing logical interfaces.

Command	**interface range** { *port-range* | **macro** *macro_name* }
Parameter Description	*port-range*: Indicates the type and ID range of interfaces. These interfaces can be Ethernet physical ports, AP ports, SVIs, or loopback interfaces. *macro_name*: Indicates the name of the interface range macro.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	● If logical interfaces are not created yet, run this command to create these interfaces and enter interface configuration mode. ● For multiple physical ports or existing logical interfaces, run this command to enter interface configuration mode. ● Use the **default** form of the command to restore default settings of these interfaces in interface configuration mode. ● Before using a macro, run the **define interface-range** command to define the interface range as a macro name in global configuration mode, and then run the **interface range macro** *macro_name* command to apply the macro.

Configuring Interface Index Persistence

- Optional.
- Run this command when the interface indexes must remain unchanged after the device is restarted.

Command	**snmp-server if-index persist**
Parameter Description	N/A
Defaults	By default, interface index persistence is disabled.
Command Mode	Global configuration mode
Usage Guide	After this command is executed, current indexes of all interfaces will be saved, and the indexes remain

	unchanged after the device is restarted. You can use the **no** or **default** form of the command to disable the interface index persistence function.

Configuring the Description of an Interface

- Optional.
- Run this command to configure the description of an interface.

Command	**description** *string*
Parameter Description	*string:* Indicates a string of up to 80 characters.
Defaults	By default, no description is configured.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the description of an interface. You can use the **no** or **default** form of the command to delete the description of an interface.-

Configuring the Link Trap Function of an Interface

- Optional.
- Run this command to obtain the link traps through SNMP.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, the link trap function is enabled.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the link trap function on an interface. When this function is enabled, the SNMP sends link traps when the link status changes on the interface. You can use the **no** or **default** form of the command to disable the link trap function.

Configuring the Administrative Status of an Interface

- Optional.
- Run this command to enable or disable an interface.
- An interface cannot send or receive packets after it is disabled.

Command	**shutdown**
Parameter Description	N/A
Defaults	By default, the administrative status of an interface is Up.
Command Mode	Interface configuration mode

Usage Guide	You can run the **shutdown** command to disable an interface, or the **no shutdown** command to enable an interface. In some cases, for example, when an interface is in errdisable state, you cannot run the **no shutdown** command on an interface. You can use the **no** or **default** form of the command to enable the interface.

Configuring Port Flapping Protection

- Optional.
- Run this command to protect the port against flapping.

Command	**physical-port dither protect**
Parameter Description	N/A
Defaults	By default, port flapping protection is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Syslog Function

- Optional.
- Run this command to enable or disable the syslog function on an interface.

Command	**[no] logging [link-updown | error-frame | link-dither]**
Parameter Description	N/A
Defaults	By default, the syslog function is enabled on an interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Configuring a Specified Interface

- Run the **interface** command. If you can enter interface configuration mode, the configuration is successful.
- For a logical interface, after the **no interface** command is executed, run the **show running** or **show interfaces** command to check whether the logical interface exists. If not, the logical interface is deleted.
- After the **default interface** command is executed, run the **show running** command to check whether the default settings of the corresponding interface are restored. If yes, the operation is successful.

Configuring Interfaces Within a Range

- Run the **interface range** command. If you can enter interface configuration mode, the configuration is successful.

- After the **default interface range** command is executed, run the **show running** command to check whether the default settings of the corresponding interfaces are restored. If yes, the operation is successful.

Configuring Interface Index Persistence

- After the **snmp-server if-index persist** command is executed, run the **write** command to save the configuration, restart the device, and run the **show interface** command to check the interface index. If the index of an interface remains the same after the restart, interface index persistence is enabled.

Configuring the Link Trap Function of an Interface

- Remove and then insert the network cable on a physical port, and enable the SNMP server. If the SNMP server receives link traps, the link trap function is enabled.
- Run the **no** form of the **snmp trap link-status** command. Remove and then insert the network cable on a physical port. If the SNMP server does not receive link traps, the link trap function is disabled.

Configuring the Administrative Status of an Interface

- Insert the network cable on a physical port, enable the port, and run the **shutdown** command on this port. If the syslog is displayed on the Console indicating that the state of the port changes to Down, and the indicator on the port is off, the port is disabled. Run the **show interfaces** command, and verify that the interface state changes to Administratively Down. Then, run the **no shutdown** command to enable the port. If the syslog is displayed on the Console indicating that the state of the port changes to Up, and the indicator on the port is on, the port is enabled.

Configuring Port Flapping Protection

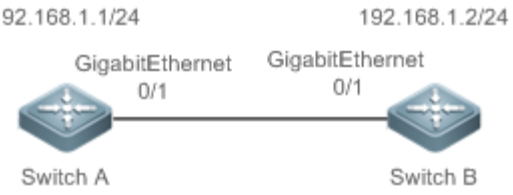
- Run the **physical-port dither protect** command in global configuration mode. Frequently remove and insert the network cable on a physical port to simulate port flapping. Verify that a syslog indicating port flapping is displayed on the Console. After such a syslog is displayed for several times, the system prompts that the port will be shut down.

Configuring the Syslog Function

- Run the **logging link-updown** command in global configuration mode to display the interface status information. Remove and then insert the network cable on a physical port. The interface state will change twice. Verify that the information is displayed on the Console, indicating that the interface state changes from Up to Down, and then from Down to Up. Run the **no logging link-updown** command. Remove and then insert the network cable. Verify that the related information is no longer displayed on the Console. This indicates that the syslog function is normal.

Configuration Example

Configuring Basic Attributes of Interfaces

Scenario **Figure 1-5**	
Configuration Steps	● Connect two devices through the switch ports. ● Configure an SVI respectively on two devices, and assign IP addresses from a 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.
A	A# configure terminal A(config)# snmp-server if-index persist A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# snmp trap link-status A(config-if-GigabitEthernet 0/1)# shutdown A(config-if-GigabitEthernet 0/1)# end A# write
B	B# configure terminal B(config)# snmp-server if-index persist B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface gigabitethernet 0/1 B(config-if-GigabitEthernet 0/1)# snmp trap link-status B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write

Verification	Perform verification on Switch A and Switch B as follows: ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether GigabitEthern 0/1 and SVI 1 are Down. ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether a trap indicating that this interface is Down is sent. ● Restart the device, and check whether the index of GigabitEthern 0/1 is the same as that before the restart.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 **GigabitEthernet 0/1 is administratively down**, line protocol is DOWN Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b) Interface address is: no ip address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0

	Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second Priority is 0 admin medium-type is Copper, oper medium-type is Copper admin duplex mode is AUTO, oper duplex is Unknown admin speed is AUTO, oper speed is Unknown flow control admin status is OFF, flow control oper status is Unknown admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Port-type: access Vlan id: 1 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets A# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP, line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) **Interface address is: 192.168.1.1/24** ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1

GigabitEthernet 0/1 is administratively down, line protocol is DOWN

Hardware is GigabitEthernet

Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b)

MTU 1500 bytes, BW 1000000 Kbit

Encapsulation protocol is Bridge, loopback not set

Keepalive interval is 10 sec, set

Carrier delay is 2 sec

Rxload is 1/255, Txload is 1/255

Queue	Transmitted packets	Transmitted bytes	Dropped packets	Dropped bytes
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	4	440	0	0

Switchport attributes:

interface's description:""

lastchange time:0 Day:20 Hour:15 Minute:22 Second

Priority is 0

admin medium-type is Copper, oper medium-type is Copper

admin duplex mode is AUTO, oper duplex is Unknown

admin speed is AUTO, oper speed is Unknown

flow control admin status is OFF, flow control oper status is Unknown

admin negotiation mode is OFF, oper negotiation state is ON

Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF

Port-type: access

Vlan id: 1

10 seconds input rate 0 bits/sec, 0 packets/sec

10 seconds output rate 0 bits/sec, 0 packets/sec

4 packets input, 408 bytes, 0 no buffer, 0 dropped

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

4 packets output, 408 bytes, 0 underruns, 0 dropped

0 output errors, 0 collisions, 0 interface resets

B# show interfaces vlan 1

Index(dec):4097 (hex):1001

VLAN 1 is UP, line protocol is DOWN

Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)

Interface address is: 192.168.1.2/24

ARP type: ARPA, ARP Timeout: 3600 seconds

MTU 1500 bytes, BW 1000000 Kbit

Encapsulation protocol is Ethernet-II, loopback not set

Keepalive interval is 10 sec, set

Carrier delay is 2 sec

Rxload is 0/255, Txload is 0/255

1.4.2 Configuring Interface Attributes

Configuration Effect

- Enable the device to connect and communicate with other devices through the switch port or routed port.
- Adjust various interface attributes on the device.

Configuration Steps

↘ Configuring a Routed Port

- Optional.
- Run this command to configure a port as a L3 routed port.
- After a port is configured as a L3 routed port, L2 protocols running on the port do not take effect.

- This command is applicable to a L2 switch port.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an Ethernet physical port is a L2 switch port.
Command Mode	Interface configuration mode
Usage Guide	On a L3 device, you can run this command to configure a L2 switch port as a L3 routed port. You can run the **switchport** command to change a L3 routed port into a L2 switch port.

Configuring a L3 AP Port

- Optional.
- Run the **no switchport** command in interface configuration mode to configure a L2 AP port as a L3 AP port. Run the **switchport** command to configure a L3 AP port as a L2 AP port.
- After a port is configured as a L3 routed port, L2 protocols running on the port do not take effect.
- This command is applicable to a L2 AP port.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an AP port is a L2 AP port.
Command Mode	Interface configuration mode
Usage Guide	After entering configuration mode of a L2 AP port on a L3 device, you can run this command to configure a L2 AP port as a L3 AP port. After entering configuration mode of a L3 AP port, you can run the **switchport** command to change a L3 AP port into a L2 AP port.

Configuring the Medium Type of an Interface

- Optional.
- Port flapping may occur if the configured medium type of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**medium-type** { **auto-select** [**prefer** [**fiber | copper**]] **| fiber | copper** }
Parameter Description	**auto-select**: Indicates that the medium type is selected automatically. **prefer** [**fiber** | **copper**]: Indicates the medium type that will be preferentially selected. **fiber**: Indicates that fiber is forcibly selected as the medium type. **copper**: Indicates that copper is forcibly selected as the medium type.
Defaults	By default, the medium type of an interface is copper.
Command Mode	Interface configuration mode
Usage Guide	Select either fiber or copper as the medium type of a port when both medium types are available. Once the medium type is selected, all interface attributes, including the status, duplex mode, and speed, are configured for the interface of the selected medium type. If the interface type is changed, the attributes of the

	new interface type are the default attributes. You can reconfigure these attributes as required. If you enable automatic selection of the medium type, the device uses the current medium if only one medium is available. If both media are available, the device uses the preferred medium as configured. By default, the preferred medium is copper. You can run the **medium-type auto-select prefer fiber** command to configure fiber as the preferred media. In automatic medium selection mode, the interface adopts the default settings of attributes, such as the speed, duplex mode, and flow control mode.

Configuring the Speed of an Interface

- Optional.
- Port flapping may occur if the configured speed of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**speed** [**10** | **100** | **1000** | **auto**]
Parameter Description	**10**: Indicates that the speed of the interface is 10 Mbps. **100**: Indicates that the speed of the interface is 100 Mbps. **1000**: Indicates that the speed of the interface is 1000 Mbps. **auto**: Indicates that the speed of the interface automatically adapts to the actual condition.
Defaults	By default, the speed of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	If an interface is an AP member port, the speed of this interface is determined by the speed of the AP port. When the interface exits the AP port, it uses its own speed configuration. You can run **show interfaces** to display the speed configurations. The speed options available to an interface vary with the type of the interface. For example, you cannot set the speed of an SFP interface to 10 Mbps.

Configuring the Duplex Mode of an Interface

- Optional.
- Port flapping may occur if the configured duplex mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**duplex** { **auto** | **full** | **half** }
Parameter Description	**auto**: Indicates automatic switching between full duplex and half duplex. **full**: Indicates full duplex. **half**: Indicates half duplex.
Defaults	By default, the duplex mode of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	The duplex mode of an interface is related to the interface type. You can run **show interfaces** to display the configurations of the duplex mode.

Configuring the Flow Control Mode of an Interface

- Optional.
- Generally, the flow control mode of an interface is off by default. For some products, the flow control mode is on by default.
- After flow control is enabled on an interface, the flow control frames will be sent or received to adjust the data volume when congestion occurs on the interface.
- Port flapping may occur if the configured flow control mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**flowcontrol** { **auto** | **off** | **on** }
Parameter Description	**auto**: Indicates automatic flow control. **off**: Indicates that flow control is disabled. **on**: Indicates that flow control is enabled.
Defaults	By default, flow control is disabled on an interface.
Command Mode	Interface configuration mode
Usage Guide	

Configuring the Auto Negotiation Mode of an Interface

- Optional.
- Port flapping may occur if the configured auto negotiation mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**negotiation mode** { **on** | **off** }
Parameter Description	**on**: Indicates that the auto negotiation mode is on. **off**: Indicates that the auto negotiation mode is off.
Defaults	By default, the auto negotiation mode is off.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the MTU of an Interface

- Optional.
- You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.
- This command is applicable to an Ethernet physical port or SVI.

Command	**mtu** *num*
Parameter Description	*num*: *64–9216*
Defaults	By default, the MTU of an interface is 1500 bytes.
Command	Interface configuration mode

Mode	
Usage Guide	This command is used to configure the interface MTU, that is, the maximum length of a data frame at the link layer. Currently, you can configure MTU for only a physical port or an AP port that contains one or more member ports.

Configuring the Bandwidth of an Interface

- Optional.
- Generally, the bandwidth of an interface is the same as the speed of the interface.

Command	**bandwidth** *kilobits*
Parameter Description	*kilobits*: The value ranges from 1 to 2,147,483,647. The unit is kilo bits.
Defaults	Generally, the bandwidth of an interface matches the type of the interface. For example, the default bandwidth of a gigabit Ethernet physical port is 1,000,000, and that of a 10G Ethernet physical port is 10,000,000.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Carrier Delay of an Interface

- Optional.
- If the configured carrier delay is long, it takes a long time to change the protocol status when the physical status of an interface changes. If the carrier delay is set to 0, the protocol status changes immediately after the physical status of an interface changes.

Command	**carrier-delay {[milliseconds]** ***num*** **| up [milliseconds]** ***num*** **down [milliseconds]** ***num*****}**
Parameter Description	*num*: The value ranges from 0 to 60. The unit is second. ***milliseconds***: Indicates the carrier delay. The value ranges from 0 to 60,000. The unit is millisecond. ***Up***: Indicates the delay after which the state of the DCD changes from Down to Up. ***Down***: Indicates the delay after which the state of the DCD changes from Up to Down.
Defaults	By default, the carrier delay of an interface is 2s.
Command Mode	Interface configuration mode
Usage Guide	If millisecond is used as the unit, the configured carrier delay must be an integer multiple of 100 milliseconds.

Configuring the Load Interval of an Interface

- Optional.
- The configured load interval affects computation of the average packet rate on an interface. If the configured load interval is short, the average packet rate can accurately reflect the changes of the real-time traffic.

Command	**load-interval** *seconds*

Parameter Description	*seconds*: The value ranges from 5 to 600. The unit is second.
Defaults	By default, the load interval of an interface is 10s.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Protected Port

- Optional.
- L2 packets cannot be forwarded between protected ports.
- This command is applicable to an Ethernet physical port or AP port.

Command	**switchport protected**
Parameter Description	N/A
Defaults	By default, no protected port is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Blocking L3 Routing Between Protected Ports

- Optional.
- After this command is configured, L3 routing between protected ports are blocked.

Command	**protected-ports route-deny**
Parameter Description	N/A
Defaults	By default, the function of blocking L3 routing between protected ports is disabled.
Command Mode	Global configuration mode
Usage Guide	By default, L3 routing between protected ports is not blocked. In this case, you can run this command to block routing between protected ports.

Configuring Port Errdisable Recovery

- Optional.
- By default, a port will be disabled and will not be recovered after a violation occurs. After port errdisable recovery is configured, a port in errdisable state will be recovered and enabled.

Command	**errdisable recovery [interval** *time***]**
Parameter Description	*time*: Indicates the automatic recovery time. The value ranges from 30 to 86,400. The unit is second.
Defaults	By default, port errdisable recovery is disabled.

Command Mode	Global configuration mode
Usage Guide	By default, a port in errdisable state is not recovered. You can recover the port manually or run this command to automatically recover the port.

Configuring Optical Module Alarm Detection

- Optional. When optical module alarm detection is required, you can run this command to enable this function.
- After this command is configured, the optical module alarm detection function is enabled. When an event is triggered, the alarm TRAP will be sent.

Command	**fiber alarm-detect enable**
Parameter Description	
Defaults	By default, the optical module alarm detection function is disabled.
Command Mode	Global configuration mode
Usage Guide	When the optical module alarm detection function is enabled, SNMP will send out the TRAP when an event such as optical module plugging/exception/exception recovery occurs, and vice versa.

Configuring Optical Module Alarm Detection Interval

- Optional. When it is necessary to set the optical module alarm detection interval, you can run this command to enable this function.
- You can run this command to adjust the detection interval of abnormal events

Command	**fiber alarm-detect period** *minutes*
Parameter Description	*Mins*: Alarm interval. The range is 1-1440, in minutes.
Defaults	By default, the alarm interval is 10 minutes.
Command Mode	Global configuration mode
Usage Guide	Optical module exception and exception recovery events will be notified within a period of time. Exception events will be notified periodically, while exception recovery events will be notified only once.

Configuring Optical Module Alarm Periodic Repeat Notification Mode

- Optional. You can run this command to disable the optical module alarm periodic notification function when necessary.
- You can run this command to enable or disable the exception event periodic notification function.

Command	**fiber alarm-detect repeat-mode** { **on** | **off** }
Parameter Description	**on**: Enables repeat notification mode. **off**: Disables repeat notification mode.
Defaults	By default, the repeat notification mode id enabled.
Command	Global configuration mode

Mode	
Usage Guide	Optical module exception and exception recovery events will be notified within a period of time. Exception events will be notified periodically. You can disable the periodic notification function by disabling the repeat notification mode switch.

Optical Module Antifake Detection

- (Optional) Run this command to enable optical module antifake detection when this function is required.
- Optical module antifake detection is disabled by default, and the system does not display any alarm if a non-Ruijie optical module is inserted. After this function is enabled, the system will display alarms for several times if a non-Ruijie optical module is inserted.

Command	**fiber antifake { ignore | enable }**
Parameter Description	ignore: Disables the optical module antifake detection function in global configuration mode. enable: Enables the optical module antifake detection function in global configuration mode.
Defaults	By default, optical module antifake detection is disabled.
Command Mode	Global configuration mode
Usage Guide	You can run the **fiber antifake enable** command to enable optical module antifake detection.

Configuring EEE

- Optional.
- The EEE mode of a port is enabled after this command is configured.

Command	**eee enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	By default, the EEE mode of a port is disabled. You can run this command to enable EEE, and use the no or default form of the command to disable EEE.

Verification

- Run the **show interfaces** command to display the attribute configurations of interfaces.

Command	**show interfaces** [*interface-type interface-number*] [**description | switchport | trunk**]
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. **description**: Indicates the interface description, including the link status. **switchport**: Indicates the L2 interface information. This parameter is effective only for a L2 interface. **trunk**: Indicates the Trunk port information. This parameter is effective for a physical port or an AP port.
Command Mode	Privileged EXEC mode

Usage Guide	Use this command without any parameter to display the basic interface information.

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN, line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec, set
  Carrier delay is 2 sec
  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
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: trunk
    Native vlan:1
    Allowed vlan lists:1-4094    //Allowed VLAN list of the Trunk port
    Active vlan lists:1, 3-4    //Active VLAN list (indicating that only VLAN 1, VLAN 3, and VLAN 4 are created on the device)
  Rxload is 1/255,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
```

	Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 0 packets output, 0 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

- Run the **show eee interfaces status** command to display the EEE status of an interface.

Command	**show eee interfaces** { *interface-type interface-number* | *status* }
Parameter Description	*interface-type interface-number*: Indicates the type and number of an interface. ***status*:** Indicates the EEE status of all interfaces.
Command Mode	Privileged EXEC mode
Usage Guide	If the interface is specified, the EEE status of the specified interface is displayed; otherwise, the EEE status of all interfaces is displayed.
	1. Display the EEE status of GigabitEthernet 0/1. Hostname#show eee interface gigabitEthernet 0/1 Interface : Gi0/1 EEE Support : Yes Admin Status : Enable Oper Status : Disable Remote Status : Disable Trouble Cause : Remote Disable

Interface	Indicates the interface information.
EEE Support	Indicates whether EEE is supported.
Admin Status	Indicates the administrative status.
Oper Status	Indicates the operational status.
Trouble Cause	Indicates the reason why the EEE status of an interface is abnormal.

2. Display the EEE status of all interfaces.

```
Hostname#show eee interface status
Interface EEE        Admin      Oper       Remote     Trouble
                Support Status     Status     Status     Cause
---------- ------- -------- -------- -------- --------------------
Gi0/1       Yes       Enable     Disable   Disable    Remote Disable
Gi0/2       Yes       Enable     Disable   Unknown    None
Gi0/3       Yes       Enable     Enable    Enable     None
```

	Gi0/4 Yes Enable Enable Enable None Gi0/5 Yes Enable Enable Enable None Gi0/6 Yes Enable Enable Enable None Gi0/7 Yes Enable Enable Enable None Gi0/8 Yes Enable Enable Enable None Gi0/9 Yes Enable Enable Enable None Gi0/10 Yes Enable Enable Enable None

Interface	Indicates the interface information.
EEE Support	Indicates whether EEE is supported.
Admin Status	Indicates the administrative status.
Oper Status	Indicates the operational status.
Trouble Cause	Indicates the reason why the EEE status of an interface is abnormal.

- Run the **show interfaces brief** command to display transmission rates of ports.

Command	**show interfaces** [*interface-type interface-number*] **brief [up | down]**
Parameter Description	*interface-type interface-number*: Specifies an interface. If this field is not specified, information of all ports are displayed. **up**: Indicates connected ports. **down**: indicates disconnected ports.
Command Mode	Privileged EXEC mode
Usage Guide	By running this command, brief information of ports is displayed, including port status, interface status, output and input bandwidth usage, and the number of output and input packet errors.

	1. Display the brief information of the TenGigabitEthernet 0/1 port.
	`Hostname#show interfaces TenGigabitEthernet 0/1 brief`
	`down: link down`
	`*down: administratively down`
	`disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)`
	`Interface Link Stat Protocol Stat Output Usage Input Usage inErrors outErrors`
	`-------- --------- -------------- -------------- ------------- ---------- ----------`
	`Te0/1 disabled down 0.00% 0.00% 0 0`
	2. Display the brief information of all connected ports.
	`Hostname#show interfaces brief up`
	`down: link down`

```
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Protocol Stat  Output Usage  Input Usage  inErrors  outErrors
---------  ---------  -------------  ------------  -----------  --------  ---------
Te0/1      up         up             83.40%        78.20%       0         0
Te0/2      up         up             82.00%        73.40%       0         0
```

3. Displays the brief information of all the ports.

```
Hostname#show interfaces brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Protocol Stat  Output Usage  Input Usage  inErrors  outErrors
---------  ---------  -------------  ------------  -----------  --------  ---------
Te0/1      down       down           0.00%         0.00%        0         0
Te0/2      down       down           0.00%         0.00%        0         0
Te0/3      down       down           0.00%         0.00%        0         0
Te0/4      down       down           0.00%         0.00%        0         0
Te0/5      down       down           0.00%         0.00%        0         0
Te0/6      down       down           0.00%         0.00%        0         0
Te0/7      down       down           0.00%         0.00%        0         0
Te0/8      down       down           0.00%         0.00%        0         0
Te0/9      down       down           0.00%         0.00%        0         0
Te0/10     disabled   down           0.00%         0.00%        0         0
```

- Run the **show interfaces ethernet brief** command to display transmission rates of ports.

Command	**show interfaces** [*interface-type interface-number*] **ethernet brief [up | down]**
Parameter Description	*interface-type interface-number*: Specifies an interface. If this field is not specified, information of all ports are displayed. **up**: Indicates connected ports. **down**: indicates disconnected ports.
Command Mode	Privileged EXEC mode
Usage Guide	By running this command, brief information of all physical, aggregation and management ports is displayed, including status, VLANs, auto negotiation, duplex mode, speed, bandwidth usage, and description.

1. Displaythe brief information of the GigabitEthernet 0/1 port.

```
Hostname#show interfaces TenGigabitEthernet 0/1 ethernet brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output Usage   Description
---------  ---------  ----  --------  -------  -------  -----------  -------------  -----------
Gi0/1       down       1     OFF       Unknown  Unknown  0.00%        0.00%          10G port
```

2. Displaythe brief information of all connected ports.

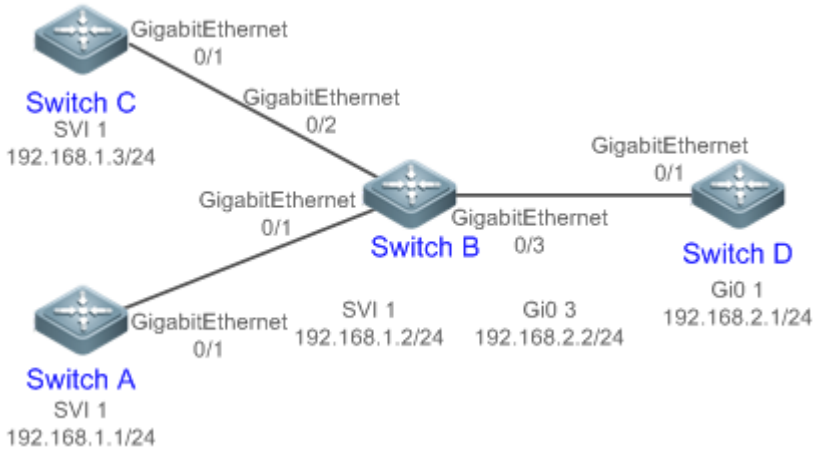
```
Hostname#show interfaces ethernet brief up
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output Usage   Description
---------  ---------  ----  --------  -------  -------  -----------  -------------  -----------
Gi0/1         UP       1     OFF       Full     1000M     79.77%       79.77%          10G port
```

3. Displays the brief information of all the ports.

```
Hostname#show interfaces ethernet brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output Usage   Description
---------  ---------  ----  --------  -------  -------  -----------  -------------  -----------
Gi0/1        *down       1     OFF       Unknown  Unknown  0.00%        0.00%          10G port
Gi0/2         down       1     OFF       Unknown  Unknown  0.00%        0.00%
Gi0/3         down       1     OFF       Unknown  Unknown  0.00%        0.00%
Ag1           up         1     OFF       Full     1000M    46.78%       46.77%
Mg0           up       routed  --        Full     1000M    --           --                IP
management Console
```

Configuration Example

Configuring Interface Attributes

Scenario **Figure 1-6**	
Configuration Steps	● On Switch A, configure GigabitEthernet 0/1 as an access mode, and the default VLAN ID is 1. Configure SVI 1, assign an IP address to SVI 1, and set up a route to Switch D. ● On Switch B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as Trunk ports, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed port, and assign an IP address from another network segment to this port. ● On Switch C, configure GigabitEthernet 0/1 as an Access port, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. ● On Switch D, configure GigabitEthernet 0/1 as a routed port, assign an IP address to this port, and set up a route to Switch A.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode access A(config-if-GigabitEthernet 0/1)# switchport access vlan 1 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# switchport mode trunk B(config-if-GigabitEthernet 0/1)# exit

	B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# switchport mode trunk B(config-if-GigabitEthernet 0/2)# exit B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)# no switchport B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/3)# exit
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# port-group 1 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface aggregateport 1 C(config-if-AggregatePort 1)# switchport mode access C(config-if-AggregatePort 1)# switchport access vlan 1 C(config-if-AggregatePort 1)# exit C(config)# interface vlan 1 C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0 C(config-if-VLAN 1)# exit
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# no switchport D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2
Verification	Perform verification on Switch A, Switch B, Switch C, and Switch D as follows: ● On Switch A, ping the IP addresses of interfaces of the other three switches. Verify that you can access the other three switches on Switch A.. ● Verify that switch B and Switch D can be pinged mutually.

	● Verify that the interface status is correct.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF **Bridge attributes:** **Port-type: access** **Vlan id: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: **Port-type: trunk** **Native vlan: 1** **Allowed vlan lists: 1-4094** **Active vlan lists: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped

	0 output errors, 0 collisions, 0 interface resets
C	C# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
D	D# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP

	Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93) **Interface address is: 192.168.2.1/24** MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

1.5 Monitoring

Clearing

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

Description	Command
Clears the counters of a specified interface.	**clear counters** [*interface-type interface-number*]

Resets the interface hardware.	**clear interface** *interface-type interface-number*

Displaying

Displaying Interface Configurations and Status

Description	Command
Displays all the status and configuration information of a specified interface.	**show interfaces** [*interface-type interface-number*]
Displays the interface status.	**show interfaces** [*interface-type interface-number*] **status**
Displays the interface errdisable status.	**show interfaces** [*interface-type interface-number*] **status err-disable**
Displays the link status change time and count of a specified port.	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Displays the administrative and operational states of switch ports (non-routed ports).	**show interfaces** [*interface-type interface-number*] **switchport**
Displays the description and status of a specified interface.	**show interfaces** [*interface-type interface-number*] **description**
Displays the counters of a specified port, among which the displayed speed may have an error of ±0.5%.	**show interfaces** [*interface-type interface-number*] **counters**
Displays the number of packets increased in a load interval.	**show interfaces** [*interface-type interface-number*] **counters increment**
Displays statistics about error packets.	**show interfaces** [*interface-type interface-number*] **counters error**
Displays the packet sending/receiving rate of an interface.	**show interfaces** [*interface-type interface-number*] **counters rate**
Displays a summary of interface information.	**show interfaces** [*interface-type interface-number*] **counters summary**
Displays the line detection status. When a cable is short-circuited or disconnected, line detection helps you correctly determine the working status of the cable.	**show interfaces** [*interface-type interface-number*] **line-detect**
Displays the bandwidth usage of an interface.	**show interfaces** [*interface-type interface-number*] **usage**
Displays brief information of ports.	**show interfaces** [*interface-type interface-number*] **brief [up | down]**
Displays the EEE status of an interface.	**show eee interfaces** { *interface-type interface-number* | *status* }
Displays configurations.	**show running-config**

Displaying Optical Module Information

Description	Command
Displays basic information about the optical module of a specified interface.	**show interfaces** [*interface-type interface-number*] **transceiver**
Displays the fault alarms of the optical module on a specified interface. If no fault occurs, "None" is displayed.	**show interfaces** [*interface-type interface-number*] **transceiver alarm**

Displays the optical module diagnosis values of a specified interface.	**show interfaces** [*interface-type interface-number*] **transceiver diagnosis**

Line Detection

The administrator can run the **line-detect** command to check the working status of a cable. When a cable is short-circuited or disconnected, line detection helps you determine the working status of the cable.

- Only a physical port using copper as the medium supports line detection. A physical port using fiber as the medium or an AP port does not support line detection.
- When line detection is performed on an operational interface, the interface will be temporarily disconnected, and then re-connected.

Description	Command
Performs line detection in interface configuration mode. When a cable is short-circuited or disconnected, line detection helps you determine the working status of the cable.	**line-detect**

2 Configuring MAC Address

2.1 Overview

A MAC address table contains the MAC addresses, interface numbers and VLAN IDs of the devices connected to the local device.

When a device forwards a packet, it finds an output port from its MAC address table according to the destination MAC address and the VLAN ID of the packet.

After that, the packet is unicast, multicast or broadcast.

This document covers dynamic MAC addresses, static MAC addresses and filtered MAC addresses. For the management of multicast MAC addresses, please see *Configuring IGMP Snooping Configuration*.

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

2.2 Applications

Application	Description
MAC Address Learning	Forward unicast packets through MAC addresses learning.
MAC Address Change Notification	Monitor change of the devices connected to a network device through MAC address change notification.

2.2.1 MAC Address Learning

Scenario

Usually a device maintains a MAC address table by learning MAC addresses dynamically. The operating principle is described as follows:

As shown in the following figure, the MAC address table of the switch is empty. When User A communicates with User B, it sends a packet to the port GigabitEthernet 0/2 of the switch, and the switch learns the MAC address of User A and stores it in the table.

As the table does not contain the MAC address of User B, the switch broadcasts the packet to the ports of all connected devices except User A, including User B and User C.

Figure 2-1 Step 1 of MAC Address Learning

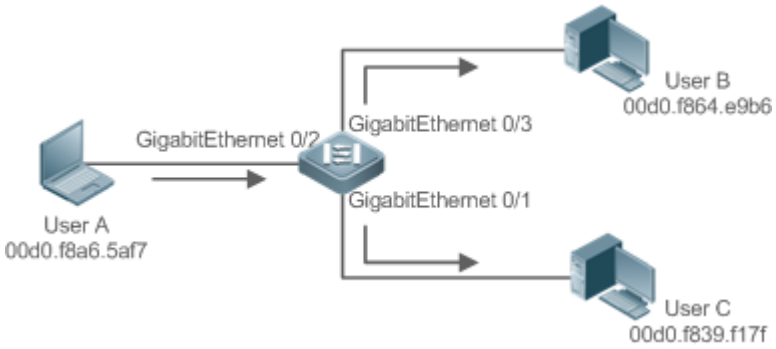


Figure 2-2 MAC Address Table 1

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2

When User B receives the packet, it sends a reply packet to User A through port GigabitEthernet 0/3 on the switch. As the MAC address of User A is already in the MAC address table, the switch send the reply unicast packet to port GigabitEthernet 0/2 port and learns the MAC address of User B. User C does not receive the reply packet from User B to User A.

Figure 2-3 Step 2 of MAC Address Learning

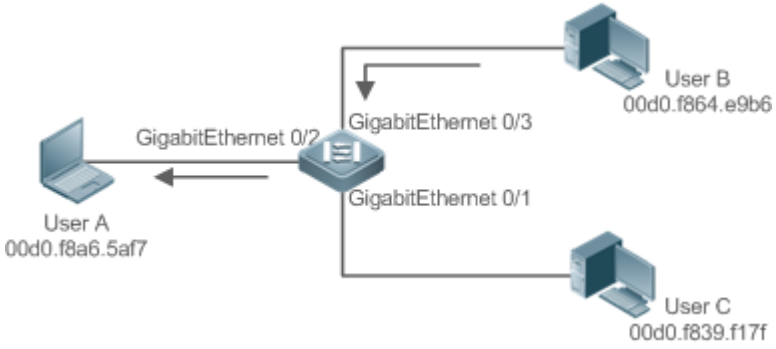


Figure 2-4 MAC Address Table 2

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Dynamic	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

Through the interaction between User A and User B, the switch learns the MAC addresses of User A and User B. After that, packets between User A and User B will be exchanged via unicast without being received by User C.

Deployment

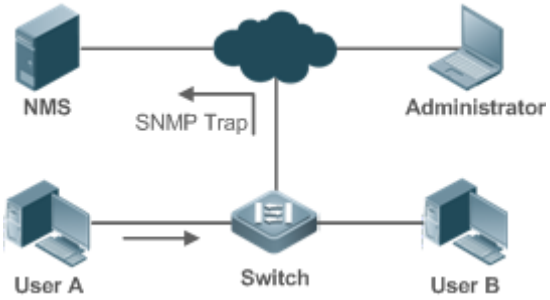
- With MAC address learning, a layer-2 switch forwards packets through unicast, reducing broadcast packets and network load.

2.2.2 MAC Address Change Notification

MAC address change notification provides a mechanism for the network management system (NMS) to monitor the change of devices connected to a network device.

Scenario

Figure 2-5 MAC Address Change Notification



After MAC address change notification is enabled on a device, the device generates a notification message when the device learns a new MAC address or finishes aging a learned MAC address, and sends the message in an SNMP Trap message to a specified NMS.

A notification of adding a MAC address indicates that a new user accesses the network, and that of deleting a MAC address indicates that a user sends no packets within an aging time and usually the user exits the network.

When a network device is connected to a number of devices, a lot of MAC address changes may occur in a short time, resulting in an increase in traffic. To reduce traffic, you may configure an interval for sending MAC address change notifications. When the interval expires, all notifications generated during the interval are encapsulated into a message.

±When a notification is generated, it is stored in the table of historical MAC address change notifications. The administrator may know recent MAC address changes by checking the table of notification history even without NMS.

A MAC address change notification is generated only for a dynamic MAC address .

Deployment

- Enable MAC address change notification on a layer-2 switch to monitor the change of devices connected to a network device.

2.3 Features

Basic Concepts

Dynamic MAC Address

A dynamic MAC address is a MAC address entry generated through the process of MAC address learning by a device.

Address Aging

A device only learns a limited number of MAC addresses, and inactive entries are deleted through address aging.

A device starts aging a MAC address when it learns it. If the device receives no packet containing the source MAC address, it will delete the MAC address from the MAC address table when the time expires.

Forwarding via Unicast

If a device finds in its MAC address table an entry containing the MAC address and the VLAN ID of a packet and the output port is unique, it will send the packet through the port directly.

Forwarding via Broadcast

If a device receives a packet containing the destination address ffff.ffff.ffff or an unidentified destination address, it will send the packet through all the ports in the VLAN where the packet is from, except the input port.

Overview

Feature	Description
Dynamic Address Limit for VLAN	Limit the number of dynamic MAC addresses in a VLAN.
Dynamic Address Limit for Interface	Limit the number of dynamic MAC addresses on an interface.

2.3.1 Dynamic Address Limit for VLAN

Working Principle

The MAC address table with a limited capacity is shared by all VLANs. The user can configure the maximum number of dynamic MAC addresses for each VLAN to prevent one single VLAN from exhausting the MAC address table space.

A VLAN can only learn a limited number of dynamic MAC addresses after the limit is configured. The packets exceeding the limit are forwarded.User can configure the maximum MAC addresses learned by a VLAN. After the maximum number exceeds the limit, the VLAN will stop learning MAC address, and packets will be discarded.

- If the number of learned MAC addresses is greater than the limit, a device will stop learning the MAC addresses from the VLAN and will not start learning again until the number drops below the limit after address aging.
- The MAC addresses copied to a specific VLAN are not subject to the limit.

2.3.2 Dynamic Address Limit for Interface

Working Principle

An interface can only learn a limited number of dynamic MAC addresses after the limit is configured. The packets exceeding the limit are forwarded.

User can configure the maximum MAC addresses learned by a VLAN. After the maximum number exceeds the limit, the VLAN will stop learning MAC address, and packets will be discarded.

- If the number of learned MAC addresses is greater than the limit, a device will stop learning the MAC addresses from the interface and will not start learning again until the number drops below the limit after address aging.

2.4 Configuration

Configuration	Description and Command	
Configuring Dynamic MAC Address	(Optional) It is used to enable MAC address learning.	
	mac-address-learning	Configures MAC address learning globally or on an interface.
	mac-address-table aging-time	Configures an aging time for a dynamic MAC address.
Configuring a Static MAC Address	(Optional) It is used to bind the MAC address of a device with a port of a switch.	
	mac-address-table static	Configures a static MAC address.
Configuring a MAC Address for Packet Filtering	(Optional) It is used to filter packets.	
	mac-address-table filtering	Configures a MAC address for packet filtering.
Configuring MAC Address Change Notification	(Optional) It is used to monitor change of devices connected to a network device.	
	mac-address-table notification	Configures MAC address change notification globally.
	snmp trap mac-notification	Configures MAC address change notification on an interface.
Configuring Maximum Number of MAC Addresses Learned by a VLAN	(Optional) It is used to configure the maximum number of MAC addresses learned by a VLAN/port.	
	max-dynamic-mac-count *count*	Configures the maximum number of MAC addresses learned by a VLAN/port.

2.4.1 Configuring Dynamic MAC Address

Configuration Effect

Learn MAC addresses dynamically and forward packets via unicast.

Configuration Steps

↘ **Configuring Global MAC Address Learning**

- Optional.
- You can perform this configuration to disable global MAC address learning.
- Configuration:

Command	**mac-address-learning** { **enable** | **disable** }
Parameter De	**enable**: Enables global MAC address learning.

scription	**disable**: Disable global MAC address learning.
Defaults	Global MAC address learning is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

By default, global MAC address learning is enabled. When global MAC address learning is enabled, the MAC address learning configuration on an interface takes effect; when the function is disabled, MAC addresses cannot be learned globally.

Configuring MAC Address Learning on Interface

- Optional.
- You can perform this configuration to disable MAC address learning on an interface.
- Configuration:

Command	**mac-address-learning**
Parameter Description	**N/A**
Defaults	MAC address learning is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	Perform this configuration on a layer-2 interface, for example, a switch port or an AP port.

By default, MAC address learning is enabled. If DOT1X, IP SOURCE GUARD, or a port security function is configured on a port, MAC address learning cannot be enabled. Access control cannot be enabled on a port with MAC address learning disabled.

Configuring an Aging Time for a Dynamic MAC Address

- Optional.
- Configure an aging time for dynamic MAC addresses.
- Configuration:

Command	**mac-address-table aging-time** *value*
Parameter Description	*value*: Indicates the aging time. The value is either 0 or in the range from 10 to 1000,000.
Defaults	The default is 300s.
Command Mode	Global configuration mode
Usage Guide	If the value is set to 0, MAC address aging is disabled and learned MAC addresses will not be aged.

The actual aging time may be different from the configured value, but it is not more than two times of the configured value.

Verification

- Check whether a device learns dynamic MAC addresses.
- Run the **show mac-address-table dynamic** command to display dynamic MAC addresses.
- Run the **show mac-address-table aging-time** command to display the aging time for dynamic MAC addresses.

Command	**show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Displays the information of a specific dynamic MAC address. **interface** *interface-id*: Specifies a physical interface or an AP port. **vlan** *vlan-id*: Displays the dynamic MAC addresses in a specific VLAN.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

```
Hostname# show mac-address-table dynamic
Vlan    MAC Address       Type            Interface
----    ------------      ------      ------------------
1       0000.0000.0001    DYNAMIC     GigabitEthernet 1/1
1       0001.960c.a740    DYNAMIC     GigabitEthernet 1/1
1       0007.95c7.dff9    DYNAMIC     GigabitEthernet 1/1
1       0007.95cf.eee0    DYNAMIC     GigabitEthernet 1/1
1       0007.95cf.f41f    DYNAMIC     GigabitEthernet 1/1
1       0009.b715.d400    DYNAMIC     GigabitEthernet 1/1
1       0050.bade.63c4    DYNAMIC     GigabitEthernet 1/1
```

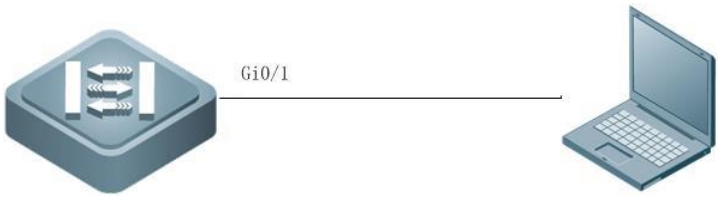
Field	Description
Vlan	Indicates the VLAN where the MAC address resides.
MAC Address	Indicates a MAC Address.
Type	Indicates a MAC address type.
Interface	Indicates the interface where the MAC address resides.

Command	**show mac-address-table aging-time**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

	Hostname# show mac-address-table aging-time **Aging time: 300**

Configuration Example

↘ Configuring Dynamic MAC Address

Scenario **Figure 2-6**	
Configuration Steps	● Enable MAC address learning on an interface. ● Configure the aging time for dynamic MAC addresses to 180s. ● Delete all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	Hostname# configure terminal Hostname(config-if-GigabitEthernet 0/1)# mac-address-learning Hostname(config-if-GigabitEthernet 0/1)# exit Hostname(config)# mac aging-time 180 Hostname# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Verification	● Check MAC address learning on an interface. ● Displaythe aging time for dynamic MAC addresses. ● Displayall dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	Hostname# show mac-address-learning **GigabitEthernet 0/1 learning ability: enable** Hostname# show mac aging-time Aging time : **180 seconds** Hostname# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1 Vlan MAC Address Type Interface ---------- ---------- -------- ---------- **1 00d0.f800.1001 STATIC GigabitEthernet 1/1**

Common Errors

Configure MAC address learning on an interface before configuring the interface as a layer-2 interface, for example, a switch port or an AP port.

2.4.2 Configuring a Static MAC Address

Configuration Effect

- Bind the MAC address of a network device with a port of a switch.

Configuration Steps

↘ Configuring a Static MAC address

- Optional.
- Bind the MAC address of a network device with a port of a switch.
- Configuration:

Command	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides. **interface** *interface-id*: Specifies a physical interface or an AP port.
Defaults	By default, no static MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	When the switch receives a packet containing the specified MAC address on the specified VLAN, the packet is forwarded to the bound interface.

Verification

- Run the **show mac-address-table static** command to check whether the configuration takes effect.

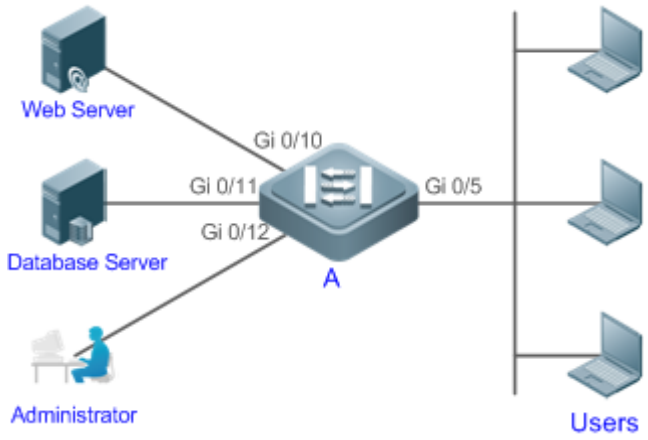
Command	**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Specifies a MAC address. **interface** *interface-id*: Specifies a physical interface or an AP port. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	Hostname# show mac-address-table static Vlan MAC Address Type Interface ----- ----------- -------- ------------------- **1 00d0.f800.1001 STATIC GigabitEthernet 1/1** **1 00d0.f800.1002 STATIC GigabitEthernet 1/1** **1 00d0.f800.1003 STATIC GigabitEthernet 1/1**

Configuration Example

Configuring a Static MAC address

In the above example, the relationship of MAC addresses, VLAN and interfaces is shown in the following table.

Role	MAC Address	VLAN ID	Interface ID
Web Server	00d0.3232.0001	VLAN2	Gi0/10
Database Server	00d0.3232.0002	VLAN2	Gi0/11
Administrator	00d0.3232.1000	VLAN2	Gi0/12

Scenario **Figure 2-7**	
Configuration Steps	● Specify destination MAC addresses (*mac-address*). ● Specify the VLAN (*vlan-id*) where the MAC addresses reside. ● Specify interface IDs (*interface-id*).
A	A# configure terminal A(config)# mac-address-table static 00d0.f800.3232.0001 vlan 2 interface gigabitEthernet 0/10 A(config)# mac-address-table static 00d0.f800.3232.0002 vlan 2 interface gigabitEthernet 0/11 A(config)# mac-address-table static 00d0.f800.3232.1000 vlan 2 interface gigabitEthernet 0/12
Verification	Display the static MAC address configuration on a switch.
A	A# show mac-address-table static Vlan MAC Address Type Interface ---------- -------------------- -------- -------------------- **2 00d0.f800.3232.0001 STATIC GigabitEthernet 0/10** **2 00d0.f800.3232.0002 STATIC GigabitEthernet 0/11** **2 00d0.f800.3232.1000 STATIC GigabitEthernet 0/12**

Common Errors

- Configure a static MAC address before configuring the specific port as a layer-2 interface, for example, a switch port or an AP port.

2.4.3 Configuring a MAC Address for Packet Filtering

Configuration Effect

- If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Configuration Steps

↘ **Configuring a MAC Address for Packet Filtering**

- Optional.
- Perform this configuration to filter packets.
- Configuration:

Command	**mac-address-table filtering** *mac-address* **vlan** *vlan-id*
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Defaults	By default, no filtered MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Verification

- Run the **show mac-address-table filter** command to display the filtered MAC address.

Command	**show mac-address-table filter** [**address** *mac-address*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	Hostname# show mac-address-table filtering Vlan MAC Address Type Interface ------ -------------------- -------- ----------- **1 0000.2222.2222 FILTER**

Configuration Example

Configuring a MAC Address for Packet Filtering

Configuration Steps	● Specify a destination MAC address (*mac-address*) for filtering. ● Specify a VLAN where the MAC addresses resides.
	Hostname# configure terminal Hostname(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1
Verification	Display the filtered MAC address configuration.
	Hostname# show mac-address-table filter Vlan MAC Address Type Interface ---------- ---------- -------- ---------- **1 00d0.f800.3232.0001 FILTER**

2.4.4 Configuring MAC Address Change Notification

Configuration Effect

- Monitor change of devices connected to a network device.

Configuration Steps

Configuring NMS

- Optional.
- Perform this configuration to enable an NMS to receive MAC address change notifications.
- Configuration:

Command	**snmp-server host** *host-addr* **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*
Parameter Description	**host** *host-addr*: Specifies the IP address of a receiver. **version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }: Specifies the version of SNMP TRAP messages. You can also specify authentication and a security level for packets of Version 3. *community-string*: Indicates an authentication name.
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling SNMP Trap

- Optional.
- Perform this configuration to send SNMP Trap messages.
- Configuration:

Command	**snmp-server enable traps**
Parameter Description	N/A
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Global MAC Address Change Notification

- Optional.
- If MAC address change notification is disabled globally, it is disabled on all interfaces.
- Configuration:

Command	**mac-address-table notification**
Parameter Description	N/A
Defaults	By default, MAC address change notification is disabled globally.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring MAC Address Change Notification On Interface

- Optional.
- Perform this configuration to enable MAC address change notification on an interface.
- Configuration:

Command	**snmp trap mac-notification** { **added** | **removed** }
Parameter Description	**added**: Generates a notification when an MAC address is added. **removed**: Generates a notification when an MAC address is deleted.
Defaults	By default, MAC address change notification is disabled on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Interval for Generating MAC Address Change Notifications and Volume of Notification History

- Optional.
- Perform this configuration to modify the interval for generating MAC address change notifications and the volume of notification history.

- Configuration:

Command	**mac-address-table notification** { **interval** *value* | **history-size** *value* }
Parameter Description	**interval** *value*: (Optional) Indicates the interval for generating MAC address change notifications. The value ranges from 1 to 3600 seconds,. **history-size** *value*: Indicates the maximum number of entries in the table of notification history. The value ranges from 1 to 200.
Defaults	The default interval is 1 second. The default maximum amount of notifications is 50.
Command Mode	Global configuration mode
Usage Guide	N/A

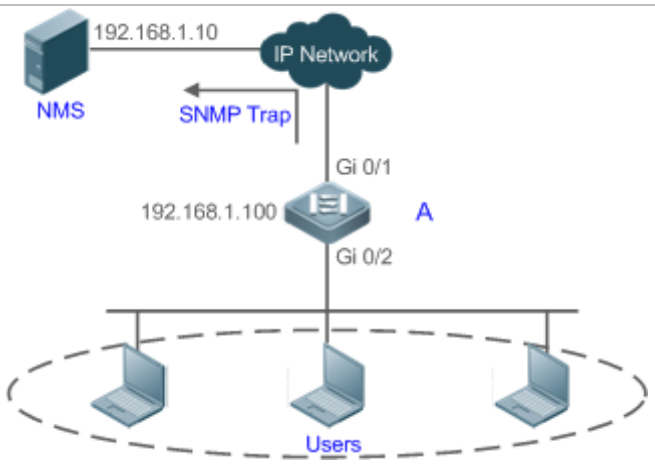
Verification

- Run the **show mac-address-table notification** command to check whether the NMS receives MAC address change notifications.

Command	**show mac-address-table notification [interface [*interface-id*] | history]**
Parameter Description	**Interface**:Displays the configuration of MAC address change notification on all interfaces. ***interface-id***: Displays the configuration of MAC address change notification on a specified interface. **history**: Displays the history of MAC address change notifications.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
Usage Guide	Display the configuration of global MAC address change notification. Hostname#show mac-address-table notification MAC Notification Feature : **Enabled** Interval(Sec): **300** Maximum History Size : **50** Current History Size : **0**

Field	Description
Interval(Sec)	Indicates the interval for generating MAC address change notifications.
Maximum History Size	Indicates the maximum number of entries in the table of notification history.
Current History Size	Indicates the current notification entry number.

Configuration Example

Scenario **Figure 2-8**	 The figure shows an intranet of an enterprise. Users are connected to A via port Gi0/2. The Perform the configuration to achieve the following effects: ● When port Gi0/2 learns a new MAC address or finishes aging a learned MAC address, a MAC address change notification is generated. ● Meanwhile, A sends the MAC address change notification in an SNMP Trap message to a specified NMS. ● In a scenario where A is connected to a number of Users, the configuration can prevent MAC address change notification burst in a short time so as to reduce the network flow.
Configuration Steps	● Enable global MAC address change notification on A, and configure MAC address change notification on port Gi0/2. ● Configure the IP address of the NMS host, and enable A with SNMP Trap. A communicates with the NMS via routing. ● Configure the interval for sending MAC address change notifications to 300 seconds (1 second by default).
A	Hostname# configure terminal Hostname(config)# mac-address-table notification Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added Hostname(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed Hostname(config-if-GigabitEthernet 0/2)# exit Hostname(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2 Hostname(config)# snmp-server enable traps Hostname(config)# mac-address-table notification interval 300
Verification	● Check whether MAC address change notification is enabled globally.

	● Check whether MAC address change notification is enabled on the interface. ● Display the MAC addresses of interfaces, and run the **clear mac-address-table dynamic** command to simulate aging dynamic MAC addresses. ● Check whether global MAC address change notification is enabled globally. ● Displaythe historyof MAC address change notifications.
A	Hostname# show mac-address-table notification MAC Notification Feature : **Enabled** Interval(Sec): **300** Maximum History Size : **50** Current History Size : **0** Hostname# show mac-address-table notification interface GigabitEthernet 0/2 Interface MAC Added Trap MAC Removed Trap ---------- ---------- ---------- GigabitEthernet 0/2 Enabled Enabled Hostname# show mac-address-table interface GigabitEthernet 0/2 Vlan MAC Address Type Interface ---------- ---------- -------- ---------- 1 00d0.3232.0001 DYNAMIC GigabitEthernet 0/2 Hostname# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 1 Hostname# show mac-address-table notification history History Index : 0 Entry Timestamp: 221683 MAC Changed Message : Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2

2.4.5 Configuring the Maximum Number of MAC Addresses Learned by a Port

Configuration Effect

- Only a limited number of dynamic MAC addresses can be learned by a port.

Notes

None

Configuration Steps

Configuring the Maximum Number of MAC Addresses Learned by a Port

- Optional
- Perform this operation on the switch.

Command	**max-dynamic-mac-count** *count*
Parameter Description	**count**: Indicates the maximum number of MAC addresses learned by a port.
Defaults	By default, the number of MAC addresses learned by a port is not limited. After the number of MAC addresses learned by a port is limited and after the maximum number of MAC addresses exceeds the limit, packets from source MAC addresses are forwarded by default.
Command Mode	Interface configuration mode
Usage Guide	

Verification

- Run **show run** to query the configuration result.

Configuration Example

Configuring the Maximum Number of MAC Addresses Learned by a Port

Configuration Steps	• Configure the maximum number of MAC addresses learned by a port.
	• Configure the maximum number of MAC addresses learned by a port. Hostname(config)# interface GigabitEthernet 1/1 Hostname(config-if-GigabitEthernet 1/1)# max-dynamic-mac-count 100
Verification	Run **show running** on the switch to query the configuration.

Common Errors

None

2.5 Monitoring

Clearing

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

Description	Command
Clears dynamic MAC addresses.	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Displaying

Description	Command
Displays the MAC address table.	**show mac-address-table** { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Displays the aging time for dynamic MAC addresses.	**show mac-address-table aging-time**
Displays the maximum number of dynamic MAC addresses.	**show mac-address-table max-dynamic-mac-count**
Displays the configuration and history of MAC address change notifications.	**show mac-address-table notification [interface [** ***interface-id*** *]* **| history]**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs MAC address operation.	**debug bridge mac**

3 Configuring Aggregated Port

3.1 Overview

An aggregated port (AP) is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

An AP port supports load balancing, namely, distributes load evenly among member links. Besides, an AP port realizes link backup. When a member link of the AP port 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.

For example, the link between two devices supports a maximum bandwidth of 1,000 Mbps. 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.

For example, there are two devices connected by a 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.

Protocols and Standards

- IEEE 802.3ad

3.2 Applications

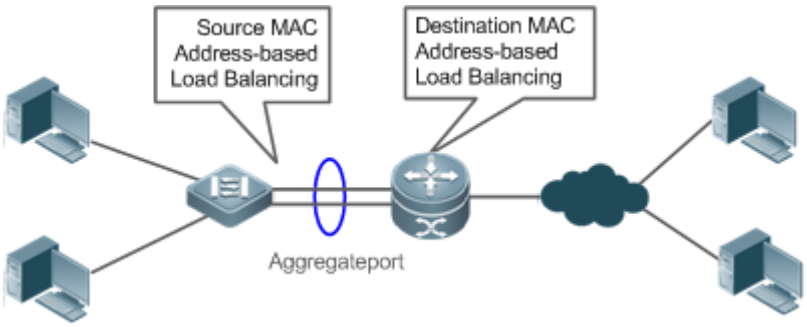
Applications	Description
AP Link Aggregation and Load Balancing	A large number of packets are transmitted between an aggregation device and a core device, which requires a greater bandwidth. To meet this requirement, you can bundle the physical links between the devices into one logical link to increase the link bandwidth, and configure a proper load balancing algorithm to distribute the work load evenly to each physical link, thus improving bandwidth utilization.

3.2.1 AP Link Aggregation and Load Balancing

Scenario

In Figure 3-1, the switch communicates with the router through an AP port. All the devices on the intranet (such as the two PCs on the left) use the router as a gateway. All the devices on the extranet (such as the two PCs on the right) send packets to the internet devices through the router, with the gateway's MAC address as its source MAC address. To distribute the load between the router and other hosts to other links, configure destination MAC address-based load balancing. On the switch, configure source MAC address-based load balancing.

Figure 3-1 AP Link Aggregation and Load Balancing



Deployment

- Configure the directly connected ports between the switch and router as a static AP port or a Link Aggregation Control Protocol (LACP) AP port.
- On the switch, configure a source MAC address-based load balancing algorithm.
- On the router, configure a destination MAC address-based load balancing algorithm.

3.3 Features

Basic Concepts

Static AP

The static AP mode is an aggregation mode in which physical ports are directly added to an AP aggregation group through manual configuration to allow the physical ports to forward packets when the ports are proper in link state and protocol state.

An AP port in static AP mode is called a static AP, and its member ports are called static AP member ports.

LACP

LACP is a protocol about dynamic link aggregation. It exchanges information with the connected device through LACP data units (LACPDUs).

An AP port in LACP mode is called an LACP AP port, and its member ports are called LACP AP member ports.

AP Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

AP member ports in active mode initiate LACP negotiation. AP member ports in passive mode only respond to received LACPDUs. AP member ports in static mode do not send LACPDUs for negotiation. The following table lists the requirements for peer port mode.

Port Mode	Peer Port Mode
Active mode	Active or passive mode
Passive mode	Active mode
Static Mode	Static Mode

AP Member Port State

There are two kinds of AP member port state available:

- 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.

There are three kinds of LACP member port state:

- 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, 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.)

Only full-duplex ports are capable of LACP aggregation.

LACP aggregation can be implemented only when the rates, flow control approaches, medium types, and Layer-2/3 attributes of member ports are consistent.

If you modify the preceding attributes of a member port in the aggregation group, LACP aggregation will fail.

The ports which are prohibited from joining or exiting an AP port cannot be added to or removed from a static AP port or an LACP AP port.

LACP System ID

One device can be configured with only one LACP aggregation system. The system is identified by a system ID and each system has a priority, which is a configurable value. The system ID consists of the LACP system priority and MAC address of the device. A lower system priority indicates a higher priority of the system ID. If the system priorities are the same, a smaller MAC address of the device indicates a higher priority of the system ID. The system with an ID of a higher priority determines the port state. The port state of a system with an ID of a lower priority keeps consistent with that of a higher priority.

LACP Port ID

Each port has an independent LACP port priority, which is a configurable value. The port ID consists of the LACP port priority and port number. A smaller port priority indicates a higher priority of the port ID. If the port priorities are the same, a smaller port number indicates a higher priority of the port ID.

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. When the new master port is not in Bundle state, LACP disaggregates the member ports and performs aggregation again.

Overview

Overview	Description
Link Aggregation	Aggregates physical links statically or dynamically to realize bandwidth extension and link backup.
Load Balancing	Balances the load within an aggregation group flexibly by using different load balancing methods.

3.3.1 Link Aggregation

Working Principle

There are two kinds of AP link aggregation. One is static AP, and the other is dynamic aggregation through LACP.

- Static AP

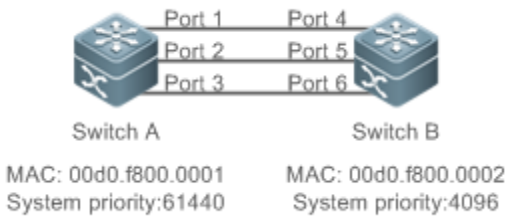
The static AP configuration is simple. Run a command to add the specified physical port to the AP port. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

- Dynamic AP (LACP)

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 3-2 LACP Negotiation



In Figure 3-2, Switch A is connected to Switch B through three ports. Set the system priorities of Switch A and Switch B to 61440 and 4096 respectively. Enable LACP on the Ports 1–6, set the aggregation mode to the active mode, and set the port priority to the default value 32768.

When receiving an LACPDU from Switch A, Switch B finds that it has a higher system ID priority than Switch A (the system priority of Switch B is higher than that of Switch A). Switch 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 Switch B, Switch A finds that Switch B has a higher system ID priority and has set Port 4, Port 5, and Port 6 to Bundle state. Then Switch A also sets Port 1, Port 2, and Port 3 to Bundle state.

3.3.2 Load Balancing

Working Principle

AP 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 Layer-4 source and destination port numbers. The packet flow with the consistent feature is transmitted by one member link, and different packet flows are evenly distributed to member links. For example, in source MAC address-based load balancing, packets are distributed to the member links based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed to member links. Packets with the identical source MAC address are forwarded by one member link.

Currently, there are several AP load balancing modes as follows:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address

Load balancing based on IP addresses or port numbers is applicable only to Layer-3 packets. When a device enabled with this load balancing method receives Layer-2 packets, it automatically switches to the default load balancing method.

All the load balancing methods use a load 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 + Layer-4 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.

Different products may support different load balancing algorithms.

3.4 Configuration

Configuration	Description and Command	
Configuring Static AP Ports	(Mandatory) It is used to configure link aggregation manually.	
	interface aggregateport	Creates an Ethernet AP port.
	port-group	Configures static AP member ports.
Configuring LACP AP Ports	(Mandatory) It is used to configure link aggregation dynamically.	

Configuration	Description and Command	
	port-group mode	Configures LACP member ports.
	lacp system-priority	Configures the LACP system priority.
	lacp port-priority	Configures the port priority.
	lacp short-timeout	Configures the short timeout mode on a port.
Enabling LinkTrap	(Optional) It is used to enable LinkTrap.	
	snmp trap link-status	Enables LinkTrap advertisement for an AP port.
	aggregateport member linktrap	Enables LinkTrap t for AP member ports.
Configuring a Load Balancing Mode	(Optional) It is used to configure a load balancing mode for an aggregated link.	
	aggregateport load-balance	Configures a load balancing algorithm for an AP port or AP member ports.

3.4.1 Configuring Static AP Ports

Configuration Effect

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.

Notes

- Only physical ports can be added to an AP port.
- The ports of different media types or port modes cannot be added to the same AP port.
- Layer-2 ports can be added to only a Layer-2 AP port, and Layer-3 ports can be added to only a Layer-3 AP port. The Layer-2/3 attributes of an AP port that contains member ports cannot be modified.
- After a port is added to an AP port, the attributes of the port are replaced by those of the AP port.
- After a port is removed from an AP port, the attributes of the port are restored.

After a port is added to an AP port, the attributes of the port are consistent with those of the AP port. Therefore, do not perform configuration on the AP member ports or apply configuration to a specific AP member port. However, some configurations (the **shutdown** and **no shutdown** commands) can be configured on AP member ports. When you use AP member ports, check whether the function that you want to configure can take effect on a specific AP member port, and perform this configuration properly.

Configuration Steps

Creating an Ethernet AP Port

- Mandatory.
- Perform this configuration on an AP-enabled device.

Command	**interface aggregateport** *ap-number*
Parameter Description	*ap-number*: Indicates the number of an AP port.
Defaults	By default, no AP port is created.
Command Mode	Global configuration mode
Usage Guide	To create an Ethernet AP port, run **interfaces aggregateport** in global configuration mode. To delete the specified Ethernet AP port, run **no interfaces aggregateport** *ap-number* in global configuration mode.

Run **port-group** to add a physical port to a static AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.

Run port-group mode to add a physical port to an LACP AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.

The AP feature must be configured on the devices at both ends of a link and the AP mode must be the same (static AP or LACP AP).

Configuring Static AP Member Ports

- Mandatory.
- Perform this configuration on AP-enabled devices.

Command	**port-group** *ap-number*
Parameter Description	**port-group** *ap-number*: Indicates the number of an AP port.
Defaults	By default, no ports are added to any static AP port.
Command Mode	Interface configuration mode of the specified Ethernet port
Usage Guide	To add member ports to an AP port, run **port-group** in interface configuration mode. To remove member ports from an AP port, run **no port-group** in interface configuration mode.

The static AP member ports configured on the devices at both ends of a link must be consistent.

After a member port exits the AP port, the default settings of the member port are restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an AP port.

After a member port exits an AP port, the port is disabled by using the **shutdown** command to avoid loops. After you confirm that the topology is normal, run **no shutdown** in interface configuration mode to enable the port again.

Converting Layer-2 APs to Layer-3 APs

- Optional.

- When you need to enable Layer-3 routing on an AP port, for example, to configure IP addresses or static route entries, convert the Layer-2 AP port to a Layer-3 AP port and enable routing on the Layer-3 AP port.
- Perform this configuration on AP-enabled devices that support Layer-2 and Layer-3 features.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, the AP ports are Layer-2 AP ports.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	The Layer-3 AP feature is supported by only Layer-3 devices.

The AP port created on a Layer-3 device that does not support Layer-2 feature is a Layer-3 AP port. Otherwise, the AP port is a Layer-2 AP port.

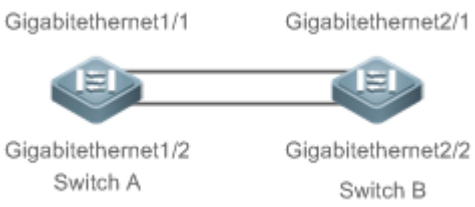
Verification

- Run **show running** to display the configuration.
- Run **show aggregateport summary** to display the AP configuration.

Command	**show aggregateport** *aggregate-port-number* [**load-balance	summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on all AP ports is displayed if you do not specify the AP port number.
	Hostname# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring an Ethernet Static AP Port

Scenario Figure 3-3	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3.

Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3
Verification	● Run **show aggregateport summary** to check whether AP port 3 contains member ports GigabitEthernet 1/1 and GigabitEthernet 1/2.
Switch A	SwitchA# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag3** 8 Enabled ACCESS **Gi1/1,Gi1/2**
Switch B	SwitchB# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag3** 8 Enabled ACCESS **Gi2/1,Gi2/2**

3.4.2 Configuring LACP AP Ports

Configuration Effect

- Connected devices perform autonegotiation through LACP to realize dynamic link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.
- It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.

Notes

- After a port exits an LACP AP port, the default settings of the port may be restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an LACP AP port.
- 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.

Configuration Steps

Configuring LACP Member Ports

- Mandatory.
- Perform this configuration on LACP-enabled devices.

Command	**port-group** *key-number* **mode** { **active | passive** }
Parameter Description	*Key-number*: Indicates the management key of an AP port. In other words, it is the LACP AP port number. The maximum value is subject to the number of AP ports supported by the device. **active**: Indicates that ports are added to a dynamic AP port actively. **passive**: Indicates that ports are added to a dynamic AP port passively.
Defaults	By default, no physical ports are added to any LACP AP port.
Command Mode	Interface configuration mode of the specified physical port
Usage Guide	Use this command in interface configuration mode to add member ports to an LACP AP port.

The LACP member port configuration at both ends of a link must be consistent.

Configuring the LACP System Priority

- Optional.
- 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 selects an AP port.
- Perform this configuration on LACP-enabled devices.

Command	**lacp system-priority** *system-priority*
Parameter Description	*system-priority*: Indicates the LACP system priority. The value ranges from 0 to 65535.
Defaults	By default, the LACP system priority is 32768.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to configure the LACP system priority. All the dynamic member links share one LACP system priority. Changing the LACP system priority will affect all member links. To restore the default settings, run **no lacp system-priority** in interface configuration mode.

Configuring the Priority of an LACP Member Port

- Optional.
- 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.
- Perform this configuration on LACP-enabled devices.

Command	**lacp port-priority** *port-priority*
Parameter	*port-priority*: Indicates the priority of an LACP member port. The value ranges from 0 to 65535.

Description	
Defaults	By default, the priority of an LACP member port is 32768.
Command Mode	Interface configuration mode of the specified physical port
Usage Guide	Use this command in global configuration mode to configure the priority of an LACP member port. To restore the settings, run **no lacp port-priority** in interface configuration mode.

Configuring the Timeout Mode of LACP Member Ports

- Optional.
- When you need to implement real-time link failure detection, configure the short timeout mode. It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.
- Perform this configuration on LACP-enabled devices, such as switches.

Command	**lacp short-timeout**
Parameter Description	N/A
Defaults	By default, the timeout mode of LACP member ports is long timeout.
Command Mode	Interface configuration mode
Usage Guide	The timeout mode is supported only by physical ports. To restore the default settings, run **no lacp short-timeout** in interface configuration mode.

Verification

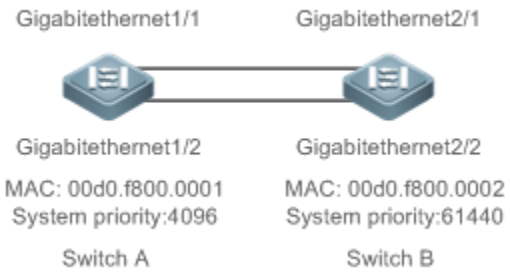
- Run **show running** to display the configuration.
- Run **show lacp summary** to display LACP link state.

Command	**show lacp summary** [*key-number*]
Parameter Description	*key-name*: Indicates the number of an LACP AP port.
Command Mode	Any mode
Usage Guide	The information on all LACP AP ports is displayed if you do not specify *key-name*.
	Hostname(config)# show lacp summary 3 System Id: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. Aggregated port 3: Local information:

```
LACP port          Oper      Port      Port
Port      Flags    State     Priority  Key       Number    State
--------------------------------------------------------------------------------
Gi0/1     SA       bndl      4096      0x3       0x1       0x3d
Gi0/2     SA       bndl      4096      0x3       0x2       0x3d
Gi0/3     SA       bndl      4096      0x3       0x3       0x3d
Partner information:
                   LACP port                    Oper      Port      Port
Port      Flags    Priority  Dev ID            Key       Number    State
--------------------------------------------------------------------------------
Gi0/1     SA       61440     00d0.f800.0001    0x3       0x1       0x3d
Gi0/2     SA       61440     00d0.f800.0001    0x3       0x2       0x3d
Gi0/3     SA       61440     00d0.f800.0001    0x3       0x3       0x3d
```

Configuration Example

Configuring LACP

Scenario **Figure 3-4**	
Configuration Steps	● On Switch A, set the LACP system priority to 4096. ● Enable dynamic link aggregation on the GigabitEthernet1/1 and GigabitEthernet1/2 ports on Switch A and add the ports to LACP AP port 3. ● On Switch B, set the LACP system priority to 61440. ● Enable dynamic link aggregation on the GigabitEthernet2/1 and GigabitEthernet2/2 ports on Switch B and add the ports to LACP AP port 3.
Switch A	SwitchA# configure terminal SwitchA(config)# lacp system-priority 4096 SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active

	SwitchA(config-if-range)# end
Switch B	SwitchB# configure terminal SwitchB(config)# lacp system-priority 61440 SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# end
Verification	● Run **show lacp summary 3** to check whether LACP AP port 3 contains member ports GigabitEthernet2/1 and GigabitEthernet2/2.
Switch A	SwitchA# 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. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi2/1 SA 32768 00d0.f800.0002 0x3 0x1 0x3d Gi2/2 SA 32768 00d0.f800.0002 0x3 0x2 0x3d
Switch B	SwitchB# show LACP summary 3 System Id: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.

Aggregated port 3:

Local information:

Port	Flags	State	LACP port Priority	Key	Oper Port Number	Port State
Gi2/1	SA	bndl	32768	0x3	0x1	0x3d
Gi2/2	SA	bndl	32768	0x3	0x2	0x3d

Partner information:

Port	Flags	LACP port Priority	Dev ID	Key	Oper Port Number	Port State
Gi1/1	SA	32768	00d0.f800.0001	0x3	0x1	0x3d
Gi1/2	SA	32768	00d0.f800.0001	0x3	0x2	0x3d

3.4.3 Enabling LinkTrap

Configuration Effect

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

Configuration Steps

↘ Enabling LinkTrap for an AP Port

- Optional.
- Enable LinkTrap in interface configuration mode. By default, LinkTrap is enabled. LinkTrap messages are sent when the link state or protocol state of the AP port is changed.
- Perform this configuration on AP-enabled devices.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, LinkTrap is enabled.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	Use this command in interface configuration mode to enable LinkTrap for the specified AP port. After LinkTrap is enabled, LinkTrap messages are sent when the link state of the AP port is changed. Otherwise, LinkTrap messages are not sent. By default, LinkTrap is enabled. To disable LinkTrap for an AP port, run **no snmp trap link-status** in interface configuration mode. LinkTrap cannot be enabled for a specific AP member port. To enable LinkTrap for all AP member ports, run **aggregateport member linktrap** in global configuration mode.

↘ Enabling LinkTrap for AP Member Ports

- Optional.
- By default, LinkTrap is disabled for AP member ports.
- Perform this configuration on AP-enabled devices.

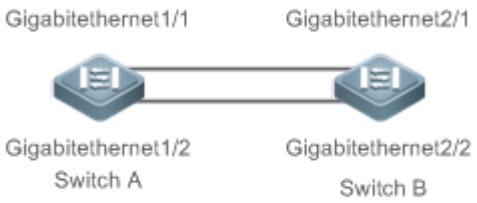
Command	**aggregateport member linktrap**
Parameter Description	N/A
Defaults	By default, LinkTrap is disabled for AP member ports.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to enable LinkTrap for all AP member ports. By default, LinkTrap messages are not sent when the link state of AP member ports is changed. To disable LinkTrap for all AP member ports, run **no aggregateport member linktrap** in global configuration mode.

Verification

- Run **show running** to displaythe configuration.
- After LinkTrap is enabled, you can monitor this feature on AP ports or their member ports by using the MIB software.

Configuration Example

Enabling LinkTrap for AP Member Ports

Scenario **Figure 3-5**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ● On Switch A, disable LinkTrap for AP port 3 and enable LinkTrap for its member ports. ● On Switch B, disable LinkTrap for AP port 3 and enable LinkTrap its AP member ports.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport member linktrap SwitchA(config)# interface Aggregateport 3 SwitchA(config-if-AggregatePort 3)# no snmp trap link-status
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport member linktrap SwitchB(config)# interface Aggregateport 3 SwitchB(config-if-AggregatePort 3)# no snmp trap link-status
Verification	● Run **show running** to check whether LinkTrap is enabled for AP port 3 and its member ports.
Switch A	SwitchA# show run | include AggregatePort 3

	Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchA# show run | include AggregatePort aggregateport member linktrap
Switch B	SwitchB# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchB# show run | include AggregatePort aggregateport member linktrap

3.4.4 Configuring a Load Balancing Mode

Configuration Effect

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 type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

Notes

Configuration Steps

↘ **Configuring the Global Load Balancing Algorithm of an AP port**

- (Optional) Perform this configuration when you need to optimize load balancing.
- Perform this configuration on AP-enabled devices.

Command	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** }
Parameter Description	**dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming packets. **src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming packets. **src-dst-ip**: Indicates that load is distributed based on source and destination IP addresses of incoming packets.

	dst-ip: Indicates that load is distributed based on the destination IP addresses of incoming packets. **src-ip**: Indicates that load is distributed based on the source IP addresses of incoming packets. **src-dst-mac**: Indicates that load is distributed based on source and destination MAC addresses of incoming packets.
Defaults	Load balancing can be based on source and destination MAC addresses, source and destination IP addresses (applicable to gateways), or the profile of enhanced load balancing (applicable to switches with CB line cards).
Command Mode	Global configuration mode
Usage Guide	To restore the default settings, run **no aggregateport load-balance** in global configuration mode. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run **no aggregateport load-balance** in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port.

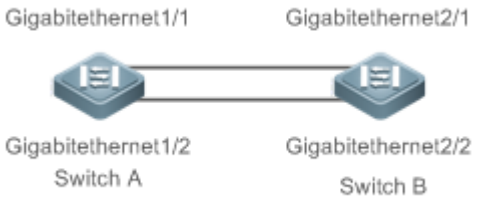
Verification

- Run **show running** to display the configuration.
- Run **show aggregateport load-balance** to display the load balancing configuration. If a device supports load balancing configuration on a specific AP port, run **show aggregateport summary** to display the configuration.

Command	**show aggregateport** *aggregate-port-number* [**load-balance	summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on All AP ports is displayed if you do not specify the AP port number.
	Hostname# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring a Load Balancing Mode

Scenario **Figure 3-6**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ● On Switch A, configure source MAC address-based load balancing for AP port 3 in global configuration mode. ● On Switch B, configure destination MAC address-based load balancing for AP port 3 in global configuration mode.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport load-balance src-mac
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport load-balance dst-mac
Verification	● Run **show aggregateport load-balance** to check the load balancing algorithm configuration.
Switch A	SwitchA# show aggregatePort load-balance Load-balance : **Source MAC**
Switch B	SwitchB# show aggregatePort load-balance Load-balance : **Destination MAC**

↘ **Configuring Hash Load Balancing Control**

Common Errors

3.5 Monitoring

Displaying

Description	Command
Displays the configuration of an enhanced load balancing profile.	**show load-balance-profile** [*profile-name*]
Displays the LACP aggregation state. You can display the information on a specified LACP AP port by specifying *key-number*.	**show lacp summary** [*key-numebr*]
Displays the summary or load balancing algorithm of an AP port.	**show aggregateport** [*ap-number*] { **load-balance** | **summary** }

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs an AP port.	**debug lsm ap**
Debugs LACP.	**debug lacp** { **packet** | **event** | **database** | **ha** | **realtime** | **stm** | **timer** | **all**}

4 Configuring VLAN

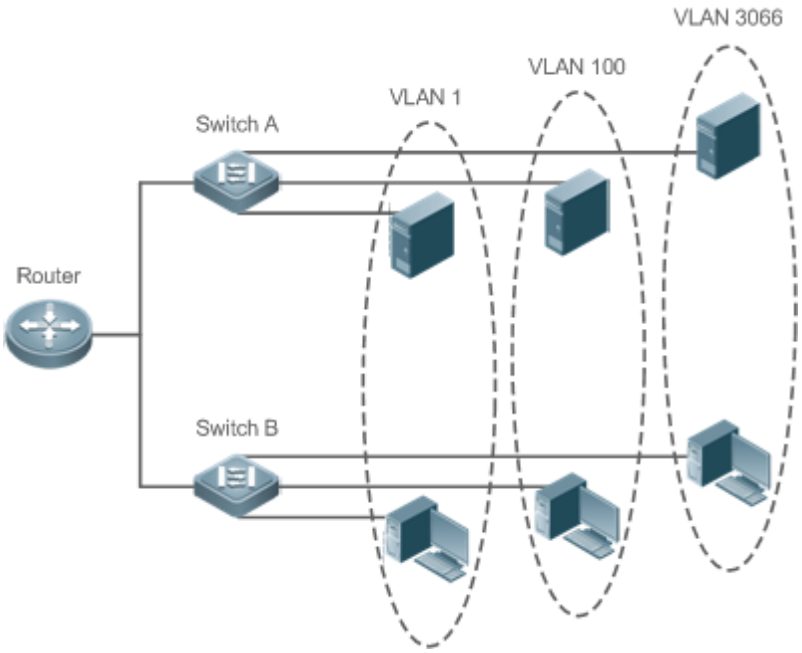
4.1 Overview

A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model.

A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices, as shown in the following figure.

Figure 4-1



Protocols and Standards

- IEEE 802.1Q

4.2 Applications

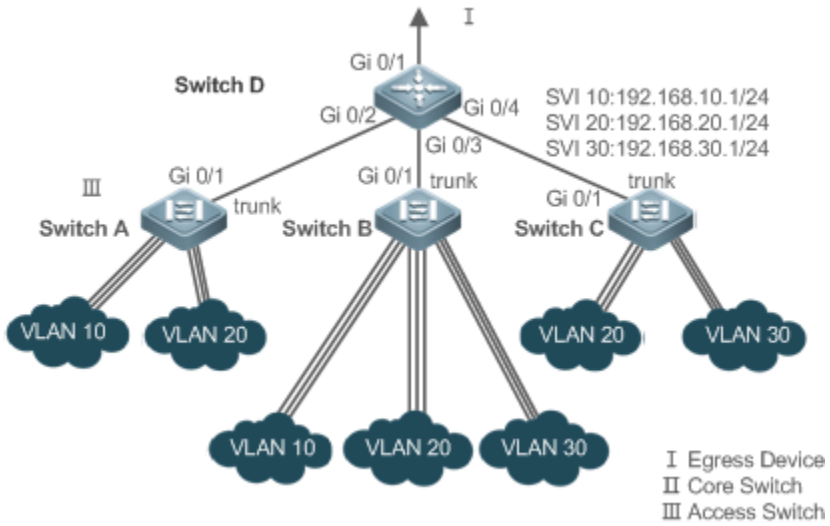
Application	Description
Isolating VLANs at Layer 2 and Interconnecting VLANs at Layer 3	An intranet is divided into multiple VLANs, realizing Layer-2 isolation and Layer-3 interconnection with each other through IP forwarding by core switches.

4.2.1 Isolating VLANs at Layer 2 and Interconnecting VLANs at Layer 3

Scenario

An intranet is divided into VLAN 10, VLAN 20 and VLAN 30, realizing Layer-2 isolation from each other. The three VLANs correspond respectively to the IP sub-networks 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, realizing interconnection with each other through IP forwarding by Layer-3 core switches.

Figure 4-2



Remarks:	Switch A, Switch B and Switch C are access switches. Configure three VLANs on a core switch and the port connected to the access switches as a Trunk port, and specify a list of allowed-VLANs to realize Layer-2 isolation; Configure three SVIs on the core switch, which are the gateway interfaces of the IP sub-networks corresponding to the three VLANs, and configure the IP addresses for these interfaces. Create VLANs respectively on the three access switches, assign Access ports for the VLANs, and specify Trunk ports of the core switch.

Deployment

- Divide an intranet into multiple VLANs to realize Layer-2 isolation among them.
- Configure SVIs on a Layer-3 switch to realize Layer-3 communication among VLANs.

4.3 Features

Basic Concepts

VLAN

A VLAN is a logical network created based on a physical network. A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

- The VLANs supported by products comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.
- The configurable VLAN IDs are from 1 to 4094.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.

Port Mode

You can determine the frames allowed to pass a port and the VLANs which the port belongs to by configuring the port mode. See the following table for details.

Port Mode	Description
Access port	An Access port belongs to only one VLAN, which is specified manually.
Trunk port (802.1Q)	A Trunk port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs or the frames of allowed-VLANs.
Uplink port	An Uplink port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs and tag the native VLAN egress traffic.
Hybrid port	A Hybrid port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs and send frames of VLANs untagged. It can also transmit frames of allowed-VLANs.

Overview

Feature	Description
VLAN	VLAN helps realize Layer-2 isolation.

4.3.1 VLAN

Every VLAN has an independent broadcast domain, and different VLANs are isolated on Layer 2.

Working Principle

Every VLAN has an independent broadcast domain, and different VLANs are isolated on Layer 2.

Layer-2 isolation: If no SVIs are configured for VLANs, VLANs are isolated on Layer 2. This means users in these VLANs cannot communicate with each other.

Layer-3 interconnection: If SVIs are configured on a Layer-3 switch for VLANs, these VLANs can communicate with each other on Layer 3.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic VLAN	(Mandatory) It is used to create a VLAN.	
	vlan	Enters a VLAN ID.
	(Optional) It is used to configure an Access port to transmit the flows from a single VLAN.	
	switchport mode access	Defines a port as a Layer-2 Access port.
	switchport access vlan	Assigns a port to a VLAN.
	add interface	Adds one Access port or a group of such ports to the current VLAN.
	(Optional) It is used to rename a VLAN.	
	name	Names a VLAN.
Configuring a Trunk Port	(Mandatory) It is used to configure the port as a Trunk port.	
	switchport mode trunk	Defines a port as a Layer-2 Trunk port.
	(Optional) It is used to configure Trunk ports to transmit flows from multiple VLANs.	
	switchport trunk allowed vlan	Configures allowed-VLANs for a Trunk port.
	switchport trunk native vlan	Specifies a native VLAN for a Trunk port.
Configuring an Uplink Port	(Mandatory) It is used to configure the port as an Uplink port.	
	switchport mode uplink	Configures a port as an Uplink port.
	(Optional) It is used to restore the port mode.	
	no switchport mode	Restores the port mode.
Configuring a Hybrid Port	(Mandatory) It is used to configure a port as a Hybrid port.	
	switchport mode hybrid	Configures a port as a Hybrid port.
	(Optional) It is used to transmit the frames of multiple VLANs untagged.	
	no switchport mode	Restores the port mode.
	switchport hybrid allowed vlan	Configures allowed-VLANs for a Hybrid port.
	switchport hybrid native vlan	Configures a default VLAN for a Hybrid port.

4.4.1 Configuring Basic VLAN

Configuration Effect

- A VLAN is identified by a VLAN ID. You may add, delete, modify VLANs 2 to 4094, but VLAN 1 is created automatically and cannot be deleted. You may configure the port mode, and add or remove a VLAN.

Notes

- N/A

Configuration Steps

↘ Creating and Modifying a VLAN

- Mandatory.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.
- Use the vlan vlan-id command to create a VLAN or enter VLAN mode.
- Configuration:

Command	**vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates VLAN ID ranging from 1 to 4094.
Defaults	VLAN 1 is created automatically and is not deletable.
Command Mode	Global configuration mode
Usage Guide	If you enter a new VLAN ID, the corresponding VLAN will be created. If you enter an existing VLAN ID, the corresponding VLAN will be modified. You may use the **no vlan** *vlan-id* command to delete a VLAN. The undeletable VLANs include VLAN1, the VLANs configured with SVIs, and SubVLANs.

↘ Renaming a VLAN

- Optional.
- You cannot rename a VLAN the same as the default name of another VLAN.
- Configuration:

Command	**name** *vlan-name*
Parameter Description	*vlan-name*: indicates a VLAN name.
Defaults	By default, the name of a VLAN is its VLAN ID. For example, the default name of the VLAN 4 is VLAN 0004.
Command Mode	VLAN configuration mode
Usage Guide	To restore the VLAN name to defaults, use the **no name** command.

↘ Assigning Current Access port to a Specified VLAN

- Optional.
- Use the **switchport mode access** command to specify Layer-2 ports (switch ports) as Access ports.
- Use the **switchport access vlan** *vlan-id* command to add an Access port to a specific VLAN so that the flows from the VLAN can be transmitted through the port.
- Configuration:

Command	**switchport mode access**
Parameter Description	N/A
Defaults	A switch port is an Access port by default.
Command Mode	Interface configuration mode
Usage Guide	N/A

Command	**switchport access vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	An Access port is added to VLAN 1 by default.
Command Mode	Interface configuration mode
Usage Guide	If a port is assigned to a non-existent VLAN, the VLAN will be created automatically.

Adding an Access Port to Current VLAN

- Optional.
- This command takes effect only on an Access port. After an Access port is added to a VLAN, the flows of the VLAN can be transmitted through the port.
- Configuration:

Command	**add interface** { *interface-id* | **range** *interface-range* }
Parameter Description	*interface-id*: indicates a single port. *interface-id*: indicates multiple ports.
Defaults	By default, all Layer-2 Ethernet ports belong to VLAN 1.
Command Mode	VLAN configuration mode
Usage Guide	In VLAN configuration mode, add a specific Access port to a VLAN. This command takes the same effect as command **switchport access vlan** *vlan-id*.

For the two commands of adding a port to a VLAN, the command configured later will overwrite the other one.

Verification

- Send untagged packets to an Access port, and they are broadcast within the VLAN.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Hostname(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- 20 VLAN0020 STATIC Gi0/1

Configuration Example

Configuring Basic VLAN and Access Port

Configuration Steps	• Create a VLAN and rename it. • Add an Access port to the VLAN. There are two approaches. One is:
	Hostname# configure terminal Hostname(config)# vlan 888 Hostname(config-vlan)# name test888 Hostname(config-vlan)# exit Hostname(config)# interface GigabitEthernet 0/3

	Hostname(config-if-GigabitEthernet 0/3)# switchport mode access Hostname(config-if-GigabitEthernet 0/3)# switchport access vlan 20 The other approach is adding an Access port (GigabitEthernet 0/3) to VLAN20: Hostname# configure terminal SwitchA(config)#vlan 20 SwitchA(config-vlan)#add interface GigabitEthernet 0/3
Verification	Check whether the configuration is correct.
	Hostname(config-vlan)#show vlan VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- 1 VLAN0001 STATIC **20 VLAN0020 STATIC Gi0/3** **888 test888 STATIC** Hostname(config-vlan)# Hostname# show interface GigabitEthernet 0/3 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- --------- ------ ------ --------- -------------- GigabitEthernet 0/3 **enabled ACCESS 20 1 Disabled ALL** Hostname# show run !

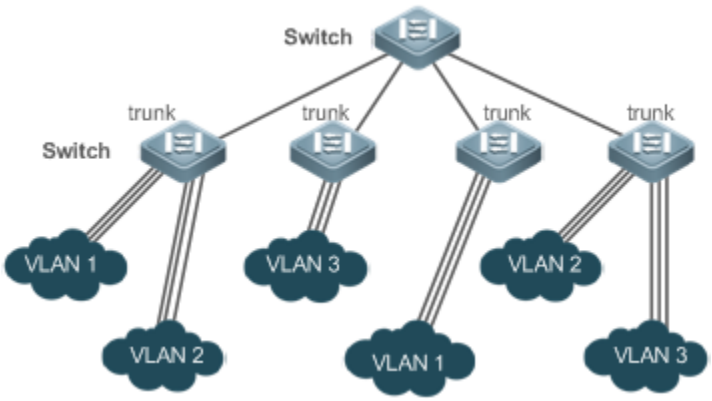
4.4.2 Configuring a Trunk Port

Configuration Effect

A Trunk is a point-to-point link connecting one Ethernet interface or multiple ones to other network devices (for example, a router or switch) and it may transmit the flows from multiple VLANs.

The Trunk of the devices adopts the 802.1Q encapsulation standard. The following figure displays a network adopting a Trunk connection.

Figure 4-3



You may configure an Ethernet port or Aggregate Port (See *Configuring Aggregate Port* for details) as a Trunk port.

You should specify a native VLAN for a Trunk port. The untagged packets received by and sent from the Trunk port are considered to belong to the native VLAN. The default VLAN ID (PVID in the IEEE 802.1Q) of this Trunk port is the native VLAN ID. Meanwhile, frames of the native VLAN sent via the Trunk are untagged. The default native VLAN of a Trunk port is VLAN 1.

When configuring a Trunk link, make sure the Trunk ports at the two ends of the link adopt the same native VLAN.

Configuration Steps

Configuring a Trunk Port

- Mandatory.
- Configure a Trunk port to transmit the flows from multiple VLANs.
- Configuration:

Command	switchport mode trunk
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Trunk.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of a Trunk port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Trunk Port

- Optional.
- By default, a trunk port transmits the flows from all the VLANs (1 to 4094). You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through a Trunk port.

- Configuration:

Command	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Parameter Description	The parameter vlan-list can be a VLAN or some VLANs, and the VLAN IDs are connected by "-" in order. For example: 10–20. **all** indicates allowed-VLANs include all VLANs; **add** indicates adding a specific VLAN to the list of allowed-VLANs; **remove** indicates removing a specific VLAN from the list of allowed-VLANs; **except** indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs. **only** indicates adding the listed VLANs to the list of allowed-VLANs, and removing the other VLANs from the list.
Defaults	The Trunk port and the Uplink port belong to all VLANs.
Command Mode	Interface configuration mode
Usage Guide	To restore the configuration on a Trunk port to defaults (**all**), use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- A Trunk port receives and sends tagged or untagged 802.1Q frames. Untagged frames transmit the flows from the native VLAN. The default native VLAN is VLAN 1.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a Trunk port.
- Configuration:

Command	**switchport trunk native vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	The default VALN for a Trunk/Uplink port is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of a Trunk port back to defaults, use the **no switchport trunk native vlan** command.

When you set the native VLAN of a port to a non-existent VLAN, this VLAN will not be created automatically. Besides, the native VLAN can be out of the list of allowed-VLANs for this port. In this case, the flows from the native VLAN cannot pass through the port.

Verification

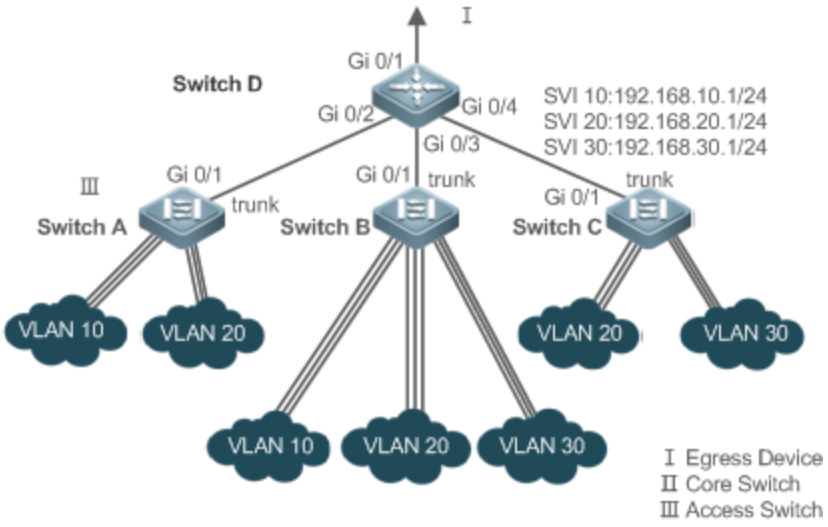
- Send tag packets to a Trunk port, and they are broadcast within the specified VLANs.

- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Hostname(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ---------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

Configuring Basic VLAN to Realize Layer-2 Isolation and Layer-3 Interconnection

Scenario Figure 4-4	
Configuration Steps	Networking Requirements: As shown in the figure above, an intranet is divided into VLAN 10, VLAN 20 and VLAN 30, realizing Layer-2 isolation from each other. The three VLANs correspond respectively to the IP sub-networks 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, realizing interconnection with each other through IP forwarding by Layer-3 core switches. Key Points: The following example describes the configuration steps on a core switch and an access switch. ● Configure three VLANs on a core switch and the port connected to the access switches as a Trunk port, and specify a list of allowed-VLANs to realize Layer-2 isolation. ● Configure three SVIs on the core switch, which are the gateway interfaces of the IP sub-networks corresponding to the three VLANs, and configure the IP addresses for these interfaces. ● Create VLANs respectively on the three access switches, assign Access ports for the VLANs, and specify Trunk ports of the core switch. The following example describes the configuration steps on

	Switch A.
D	D#configure terminal D(config)#vlan 10 D(config-vlan)#vlan 20 D(config-vlan)#vlan 30 D(config-vlan)#exit D(config)#interface range GigabitEthernet 0/2-4 D(config-if-range)#switchport mode trunk D(config-if-range)#exit D(config)#interface GigabitEthernet 0/2 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20 D(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan add 10,20,30 D(config-if-GigabitEthernet 0/3)#interface GigabitEthernet 0/4 D(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan add 20,30 D#configure terminal D(config)#interface vlan 10 D(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0 D(config-if-VLAN 10)#interface vlan 20 D(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0 D(config-if-VLAN 20)#interface vlan 30 D(config-if-VLAN 30)#ip address 192.168.30.1 255.255.255.0 D(config-if-VLAN 30)#exit
A	A#configure terminal A(config)#vlan 10 A(config-vlan)#vlan 20 A(config-vlan)#exit A(config)#interface range GigabitEthernet 0/2-12 A(config-if-range)#switchport mode access A(config-if-range)#switchport access vlan 10 A(config-if-range)#interface range GigabitEthernet 0/13-24 A(config-if-range)#switchport mode access A(config-if-range)#switchport access vlan 20 A(config-if-range)#exit A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport mode trunk
Verification	Displaythe VLAN configuration on the core switch.

	● Display VLAN information including VLAN IDs, VLAN names, status and involved ports. ● Display the status of ports Gi 0/2, Gi 0/3 and Gi 0/4.
D	D#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 VLAN0010 STATIC Gi0/2, Gi0/3** **20 VLAN0020 STATIC Gi0/2, Gi0/3, Gi0/4** **30 VLAN0030 STATIC Gi0/3, Gi0/4** D#show interface GigabitEthernet 0/2 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- ---------- ------ ------ ---------- -------------- **GigabitEthernet 0/2 enabled TRUNK 1 1 Disabled 10,20** D#show interface GigabitEthernet 0/3 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- ---------- ------ ------ ---------- -------------- **GigabitEthernet 0/3 enabled TRUNK 1 1 Disabled 10,20,30** D#show interface GigabitEthernet 0/4 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- ---------- ------ ------ ---------- -------------- **GigabitEthernet 0/4 enabled TRUNK 1 1 Disabled 20,30**

Common Errors

- N/A

4.4.3 Configuring an Uplink Port

Configuration Effect

- An Uplink port is usually used in QinQ (the IEEE 802.1ad standard) environment, and is similar to a Trunk port. Their difference is that an Uplink port only transmits tagged frames while a Trunk port sends untagged frames of the native VLAN.

Configuration Steps

↘ Configuring an Uplink Port

- Mandatory.

- Configure an Uplink port to transmit the flows from multiple VLANS, but only tagged frames can be transmitted.
- Configuration:

Command	switchport mode uplink
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Uplink.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of an Uplink port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Trunk Port

- Optional.
- You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through an Uplink port.
- Configuration:

Command	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Parameter Description	The parameter *vlan-list* can be a VLAN or some VLANs, and the VLAN IDs are connected by "-" in order. For example: 10–20. **all** indicates allowed-VLANs include all VLANs; **add** indicates adding a specific VLAN to the list of allowed-VLANs; **remove** indicates removing a specific VLAN from the list of allowed-VLANs; **except** indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs; and **only** indicates adding the listed VLANs to the list of allowed-VLANs, and removing the other VLANs from the list.
Command Mode	Interface configuration mode
Usage Guide	To restore the allowed-VLANs to defaults (**all**), use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will not be stripped when it passes an Uplink port. This is contrary to a Trunk port.
- Configuration:

Command	**switchport trunk native vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Command Mode	Interface configuration mode

Usage Guide	To restore the native VLAN of an Uplink to defaults, use the **no switchport trunk native vlan** command.

Verification

- Send tag packets to an Uplink port, and they are broadcast within the specified VLANs.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Hostname(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

Configuring an Uplink Port

Configuration Steps	The following is an example of configuring Gi0/1 as an Uplink port.
	Hostname# configure terminal Hostname(config)# interface gi 0/1 Hostname(config-if-GigabitEthernet 0/1)# switchport mode uplink Hostname(config-if-GigabitEthernet 0/1)# end
Verification	Check whether the configuration is correct.
	Hostname# show interfaces GigabitEthernet 0/1 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- --------- ------ ------ --------- ---------- GigabitEthernet 0/1 enabled **UPLINK** 1 1 disabled ALL

4.4.4 Configuring a Hybrid Port

Configuration Effect

- A Hybrid port is usually used in SHARE VLAN environment. By default, a Hybrid port is the same as a Trunk port. Their difference is that a Hybrid port can send the frames from the VLANs except the default VLAN in the untagged format.

Configuration Steps

Configuring a Hybrid Port

- Mandatory.
- Configure a Hybrid port to transmit the flows from multiple VLANs.
- Configuration:

Command	**switchport mode hybrid**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Hybrid.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of a Hybrid port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Hybrid Port

- Optional.
- By default, a Hybrid port transmits the flows from all the VLANs (1 to 4094). You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through a Hybrid port.
- Configuration:

Command	**switchport hybrid allowed vlan** [[**add** | **only**] **tagged** | [**add**] **untaged** | **remove**] *vlan_list*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	By default a Hybrid port belongs to all VLANs. The port is added to the default VLAN in untagged form and to the other VLANs in the tagged form.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a Hybrid port.
- Configuration:

Command	**switchport hybrid native vlan** *vlan_id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	The default native VLAN is VLAN 1.
Command	Interface configuration mode

Mode	
Usage Guide	To restore the native VLAN of a Hybrid port to defaults, use the **no switchport hybrid native vlan** command.

Verification

- Send tagged packets to an Hybrid port, and they are broadcast within the specified VLANs.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Hostname(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ---------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

Configuring a Hybrid Port

Configuration Steps	The following is an example of configuring Gi0/1 as a Hybrid port.
	Hostname# configure terminal Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3 Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20-30 Hostname(config-if-GigabitEthernet 0/1)# end
Verification	Check whether the configuration is correct.
	Hostname(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1 Building configuration... Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport switchport mode hybrid

	switchport hybrid **native vlan 3** switchport hybrid allowed vlan add **untagged 20-30**

4.5 Monitoring

Displaying

Description	Command
Displays VLAN configuration.	**show vlan**
Displays configuration of switch ports.	**show interface switchport**

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs VLANs.	**debug bridge vlan**

5 Configuring Voice VLAN

5.1 Overview

IP phones are widely used thanks to rapid development of technologies. The voice virtual local area network (VLAN) is a VLAN dedicated to voice data streams of users.

By creating a voice VLAN and add ports connected to voice devices to the voice VLAN, you can transmit voice data in a centralized manner in the voice VLAN, and configure Quality of Service (QoS) for voice streams to improve the transmission priority of voice streams and ensure the voice service quality.

5.2 Applications

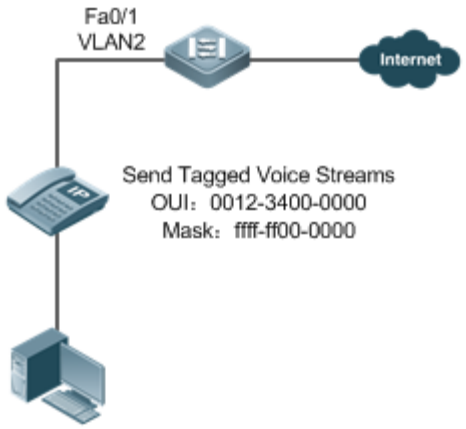
Application	Description
Configuring the Automatic Mode of the Voice VLAN	IP phones and PCs form a daisy chain and are connected to the network. Deployed IP phones can automatically obtain the IP addresses and voice VLAN information and send tagged voice streams.
Configuring the Manual Mode of the Voice VLAN	IP phones are directly connected to the network.
Isolating Voice Streams from Data Streams	PCs are connected to IP phones, and IP phones are connected to a switch. IP phones automatically obtain the IP addresses and send untagged voice streams.

5.2.1 Configuring the Automatic Mode of the Voice VLAN

Scenario

IP phones and PCs form a daisy chain and are connected to the network. Both voice and data streams are transmitted on this link. Voice streams are transmitted in the voice VLAN, whereas data streams are transmitted in the data VLAN. This ensures that voice and data streams do not interfere with each other. This networking is used when common office staff need to use PCs for data communication, and IP phones for voice communication.

Figure 5-1 Networking When the Voice VLAN Works in Automatic Mode



The Fa 0/1 port is connected to an IP phone that automatically obtains the IP address. After obtaining the IP address in the voice VLAN, the IP phone can be used normally. The Fa 0/1 port is required to forward both voice and data streams and isolate voice streams from data streams. The port can be configured as a trunk port. The native VLAN forwards data streams, whereas the voice VLAN forwards voice streams.

A device supporting the voice VLAN can check whether a stream is a voice stream of a specified voice device based on the source MAC address field in each data packet received by the port. If the source MAC address of a packet in the stream matches the Organizationally Unique Identifier (OUI) configured on the device, the stream is treated as the voice stream and transmitted in the voice VLAN.

The OUI is the first 24 bits of the MAC address. It is a globally unique identifier allocated by the Institute of Electrical and Electronics Engineers (IEEE) to an equipment supplier. You can determine the supplier of a product based on the OUI.

Deployment

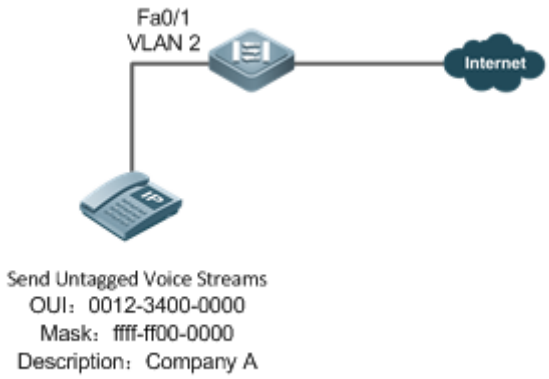
- Enable the port connected to IP phones to work in automatic mode and send tagged voice streams to devices.

5.2.2 Configuring the Manual Mode of the Voice VLAN

Scenario

An IP phone is directly connected to the voice VLAN, and only voice streams exist on the link. This type of networking is generally used when IP phones are deployed in conference rooms or when no PC is required to implement data services.

Figure 5-2 Networking When the Voice VLAN Works in Manual Mode



The deployed IP phone automatically obtains the IP address, and sends untagged voice streams. As the Fa0/1 port is connected to the IP phone that sends only untagged voice streams, and untagged voice streams do not support the automatic mode, the port can only be set to work in manual mode. The Fa0/1 port is configured as a hybrid port. According to the matching relationship requirement (see "Features"), the native VLAN of the Fa0/1 port must be a voice VLAN, and the voice VLAN must be added to the allowed untagged VLAN list of the port.

Deployment

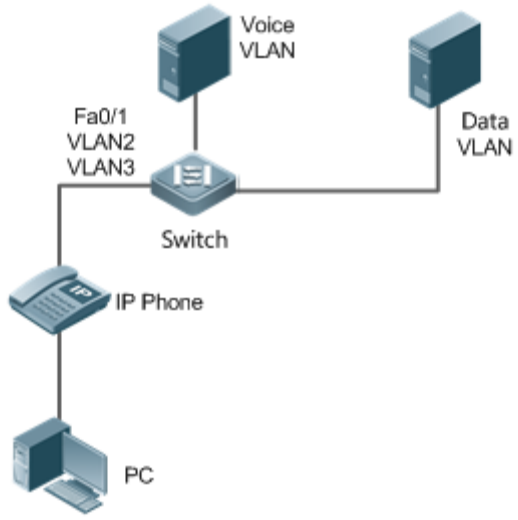
- Enable the port connected to IP phones to work in manual mode and send untagged voice streams to devices.

5.2.3 Isolating Voice Streams from Data Streams

Scenario

To ensure the quality of calls, voice data must be transmitted in the dedicated voice VLAN, and this voice VLAN cannot transmit non-voice data.

Figure 5-3 Networking That Isolates Voice Streams from Data Streams



The Fa 0/1 port is required to forward both voice and data streams and isolate voice streams from data streams. As both IP phones and PCs send untagged streams, the port must be configured as a hybrid port. The native VLAN forwards data streams, whereas the voice VLAN forwards voice streams. The IP phone connected to the Fa0/1 port sends untagged voice streams. Therefore, the voice VLAN mode must be set to the manual mode. The PC sends untagged data streams. To isolate voice streams from data streams, the MAC VLAN function must be enabled on the Fa0/1 port. The native VLAN of the Fa0/1 port is a data VLAN. In addition, to ensure that received data and voice streams are untagged, both the data VLAN and voice VLAN must be added to the allowed untagged VLAN list of the port. The security mode of the port must be disabled to ensure that data streams can be forwarded.

Deployment

- PCs are connected to IP phones, and IP phones are connected to a switch. IP phones automatically obtain the IP addresses and send untagged voice streams. The security mode is disabled on devices.

5.3 Features

Basic Concepts

Automatic and Manual Modes of the Voice VLAN

Ports in the voice VLAN can work either in automatic or manual mode. The way that ports are added to the voice VLAN varies according to the working mode.

- Automatic mode:

When a packet sent by an IP phone arrives at a device supporting the voice VLAN, the device identifies the source MAC address of the packet and compares this address with the OUI. If the source MAC address matches the OUI, the device automatically adds the input port of the voice packet to the voice VLAN, issues a policy to change the priority of the voice

packet to the priority of the voice stream in the voice VLAN configured on the device, and uses the aging mechanism to maintain ports in the voice VLAN. If the system does not receive any voice packet from an input port before the aging timer expires, the system deletes this port from the voice VLAN.

- Manual mode:

In manual port, the administrator manually adds a port to or deletes a port from the voice VLAN. The device identifies the source MAC address of the voice packet sent by the IP phone and compares this address with the OUI configured on the device. If the source MAC address matches the OUI, the device issues a policy to change the priority of the voice packet to the priority of the voice stream in the voice VLAN configured on the device.

The automatic mode is applicable to the scenario where the PC and IP phone are serially connected to the port and transmit both voice and data streams.

The manual mode is applicable to the scenario where the IP phone is directly connected to a switch and the port transmits only voice packets. In this networking mode, the port is dedicated to transmission of voice streams, which prevents data streams from affecting transmission of voice streams.

Cooperation Between Ports of the Voice VLAN and IP Phones

Based on the way that IP phones obtain IP addresses and voice VLAN information, IP phones are classified into the following types:

- The IP phone automatically obtains the IP address and the voice VLAN ID. This type of IP phones can send both tagged and untagged voice streams.
- The IP address and the voice VLAN ID are manually configured for the IP phone.

Working principle of an IP phone

Like any other network device, an IP phone needs an IP address before it can implement communication normally on the network. An IP phone obtains an IP address in either of the following ways:

- The IP address is automatically obtained through the Dynamic Host Configuration Protocol (DHCP).
- The IP address is manually configured.

When automatically obtaining an IP address, the IP phone can also request the voice VLAN information from the DHCP server. If the DHCP server returns the voice VLAN information, the IP phone can directly send the voice stream containing the voice VLAN tag. If the DHCP server does not return any voice VLAN information, the IP phone sends the voice stream without the voice VLAN tag. If the IP phone support manual configuration of the IP address and voice VLAN ID, you can manually configure the IP address and voice VLAN information on the IP hone. The IP phone sends the tagged or untagged voice streams based on your configuration.

- Voice VLAN Port and IP Phone That Sends Tagged Voice Streams

When sending the tagged voice stream, an IP hone must have obtain the voice VLAN information either automatically or through manual configuration. In this case, different types of ports must be configured accordingly so that voice packets can be transmitted normally in the voice VLAN without affecting forwarding of data streams by the switch. Unlike the IP phone that automatically obtains the voice VLAN information, the IP phone that supports manual configuration of the voice VLAN sends and receives only voice streams that contain the voice VLAN tag.

- Voice VLAN Port and IP Phone That Sends Untagged Voice Streams

An IP phone sends or receives untagged voice streams in either of the following cases:

1. The IP phone automatically obtains an IP address, but not the voice VLAN information.
2. The IP address is manually configured, but the voice VLAN information is not configured.

When the IP phone sends untagged voice streams, you must configure the default VLAN of the input port and add the default VLAN to the allowed VLAN list of the port. In addition, you must configure the default VLAN of the port as a voice VLAN so that the voice stream can be transmitted in the voice VLAN. In this case, the working mode of the voice VLAN of the port can only be set to the manual mode.

The way and process that an IP phone obtains IP address and voice VLAN information vary according to models of IP phones supplied by vendors. The working principle may differ from the preceding description. For details, see the user manual of the IP phone.

The following table describes the relationship between the working mode of the voice VLAN, IP phone type, and port type.

Working Mode of the Voice VLAN	Voice Stream Type	Port Type	Supported Or Not
Automatic mode	Tagged voice stream	Access Port	Not supported.
		Private VLAN host port	Not supported.
		Private VLAN hybrid port	Not supported.
		Trunk port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN to pass through.
		Hybrid port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN to pass through.
		Uplink port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN to pass through.
	Untagged voice stream	Access port	Not supported.
		Private VLAN host port	Not supported.
		Private VLAN hybrid port	Not supported.
		Trunk port	Not supported.
		Hybrid port	Not supported.
		Uplink port	Not supported.

Working Mode of the Voice VLAN	Voice Stream Type	Port Type	Supported Or Not
Manual mode	Tagged voice stream	Access port	Not supported.
		Private VLAN host port	Not supported.
		Private VLAN hybrid port	Not supported.
		Trunk port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN and the voice VLAN to pass through.
		Hybrid port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN to pass through, and the voice VLAN must be in the allowed tagged VLAN list of the port.
		Uplink port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN and the voice VLAN to pass through.
	Untagged voice stream	Access port	Supported. The voice VLAN must one of the VLANs to which the connected port is added.
		Private VLAN host port	Supported. The voice VLAN must be configured as the isolated VLAN or community VLAN of the port.
		Private VLAN hybrid port	Supported. The voice VLAN must be configured as the primary VLAN.
		Trunk port	Supported. The native VLAN connected to the port must be a voice VLAN, and the port allows packets of this VLAN to pass through.
		Hybrid port	Supported. The native VLAN connected to the port must be a voice VLAN. (If the MAC VLAN function is enabled on the port to isolate data streams from voice streams, the native VLAN is not necessary a voice VLAN.) In addition, the VLAN must be in the allowed untagged VLAN list of the port.

Working Mode of the Voice VLAN	Voice Stream Type	Port Type	Supported Or Not
		Uplink port	Not supported.

If an IP phone sends tagged voice streams, and the 802.1x authentication and guest VLAN functions are enabled on the port connected to the IP phone, you must allocate different VLAN IDs to the voice VLAN, default VLAN of the port, and the guest VLAN of 802.1x to ensure that these functions take effect.

The protocol VLAN takes effect on untagged packets sent by a trunk port or hybrid port. In automatic mode of the voice VLAN, a trunk port or hybrid port can process only tagged voice streams. Therefore, do not configure a VLAN both as a protocol VLAN and a voice VLAN.

If the automatic mode is used, do not set the OUI as a static address; otherwise, the automatic mode is negatively affected.

Security Mode of the Voice VLAN

To better isolate voice streams from data streams during transmission, the voice VLAN provides the security mode. When the security mode is enabled, the voice VLAN allows transmission of only voice streams. In this case, the device checks the source MAC address of each packet. When the source MAC address of a packet is a voice VLAN OUI that can be identified, the packet can be transmitted in the voice VLAN; otherwise, the packet is dropped. When the security mode is disabled, the device does not check the source MAC address of each packet, and all packets can be transmitted in the voice VLAN.

In security mode, the device checks the source MAC address of only an untagged packet or a packet containing the voice VLAN tag. For other packets that do not contain the voice VLAN tag, the device forwards or drops these packets according to the VLAN rules.

You are advised not to transmit voice and data streams concurrently in a voice VLAN. If concurrent transmission of voice and data streams is necessary, confirm that the security mode of the voice VLAN has been disabled.

Overview

Feature	Description
Voice VLAN	Transmit data streams and voice streams respectively in the data VLAN and the voice VLAN to prevent mutual interference between voice calls and data services.

5.3.1 Voice VLAN

Working Principle

A device supporting the voice VLAN transmits data streams and voice streams respectively in the data VLAN and the voice VLAN to prevent mutual interference between voice calls and data services. In addition, the device issues a priority policy to improve the priority of voice streams and ensure the quality of calls. The working principle of the voice VLAN is as follows:

Step 1: The user creates a voice VLAN dedicated to transmission of voice packets on the device, and enable the voice VLAN function on the port that is connected to the IP phone.

Step 2: Add the port connected to the IP phone to the voice VLAN. This step is crucial. The way of adding a port to the voice VLAN varies according to the working mode (automatic or manual) of the voice VLAN:

- In automatic mode, when receiving an untagged packet from the port, the device compares the source MAC address of this packet with the valid OUI. If the source MAC address matches the OUI, the packet is a voice packet. Then, the device automatically adds the port to the voice VLAN, and meanwhile learns the MAC address from this port.
- In manual mode, the user manually adds the port connected to the IP phone to the voice VLAN.

Step 3: Regardless of the working mode (automatic or manual), when a port is added to the voice VLAN, the device issues a policy to improve the priority of every packet with the source MAC address matching the OUI in the voice VLAN. For every voice packet with the source MAC address matching the OUI, the CoS is set to **6**, and DSCP is set to **46**.

After the preceding steps are complete, the port connected to the IP phone is added to the dedicated voice VLAN. Voice packets are transmitted in a centralized manner in the voice VLAN, and is forwarded to other devices with a high priority.

If the IP phone supports the Link Layer Discovery Protocol (LLDP), you do not need to configure the OUI. The device can capture the LLDP packet sent by the IP phone, and identifies the device capability field of the LLDP packet. If the device capability field is "telephone", the device extracts the source MAC address from the LLDP packet as the MAC address of the voice device. In this way, the voice device can be automatically identified.

Related Configuration

Enabling the Voice VLAN Function

By default, the voice VLAN function is disabled.

VLAN 1 cannot be configured as a voice VLAN.

Run the **vlan** *vlan-id* command to create a VLAN.

Run the **voice vlan** *vlan-id* command to enable the voice VLAN function and configure a VLAN as the voice VLAN.

Enabling the Voice VLAN Function on a Port

By default, the voice VLAN function is disabled on a port.

Run the **voice vlan enable** command to enable the voice VLAN function of a port.

Configuring the Voice VLAN Working Mode of a Port

By default, the voice VLAN working mode of a port is set to the automatic mode.

Run the **voice vlan mode auto** command to set the voice VLAN working mode of a port to the automatic mode.

Run the **no voice vlan mode auto** command to set the voice VLAN working mode of a port to the manual mode.

The voice VLAN working modes of ports are independent of each other. You can configure different voice VLAN working modes for different ports.

Configuring the Aging Time of the Voice VLAN

By default, the aging time is 1,440 minutes. The aging time takes effect on ports only in automatic mode. If the port does not receive any voice packet within the aging time, the port is automatically deleted from the voice VLAN. A longer aging time indicates that a port can reside in the voice VLAN for a longer time before it receives any voice packet.

Run the **voice vlan aging** command to configure the aging time of a port.

Configuring the OUI of the Voice VLAN

By default, the OUI is not configured.

Run the **voice vlan mac-address** command to configure the OUI of the voice VLAN that can be identified by devices.

Configuring the Security Mode of the Voice VLAN

By default, the security mode of the voice VLAN is enabled.

Run the **voice vlan security enable** command to enable the security mode of the voice VLAN.

When the security mode is enabled, only voice streams can be transmitted in the voice VLAN.

Configuring the Priority of Voice Streams in the Voice VLAN

By default, the CoS of voice streams is **6** and DSCP is **46**. A higher priority of voice streams indicates a higher priority for transmitting voice packets, which improves the quality of calls.

Run the **voice vlan security cos** command to set the CoS of voice streams in the voice VLAN.

Run the **voice vlan security dscp** command to set the DSCP of voice streams in the voice VLAN.

5.4 Configuration

Configuration Item	Description and Command	
Enabling the Voice VLAN Function	(Mandatory). It is used to globally enable the voice VLAN function.	
	voice vlan	Enables the voice VLAN function and configures a VLAN as the voice VLAN.
Enabling the Voice VLAN Function on a Port	(Mandatory). It is used to enable the voice VLAN function on a port.	
	voice vlan enable	Enables the voice VLAN function on a port.
Configuring the Aging Time of the Voice VLAN	(Optional) It is used to configure the aging time of the voice VLAN.	
	voice vlan aging	Configures the aging time of the voice VLAN. The value ranges from 5 to 10,000 minutes. The default value is 1,440 minutes.
Configuring the OUI of the	(Optional) It is used to configure the OUI of the voice VLAN.	

Configuration Item	Description and Command	
Voice VLAN	**voice vlan mac-address**	Configures the OUI of the voice VLAN that can be identified by devices.
Configuring the Security Mode of the Voice VLAN	(Optional) It is used to configure the security mode of the voice VLAN.	
	voice vlan security enable	Configures the security mode of the voice VLAN.
Configuring the Priority of Voice Streams in the Voice VLAN	(Optional) It is used to configure the priority of voice streams in the voice VLAN.	
	voice vlan cos *cos-value* **voice vlan dscp** *dscp-value*	Configures the priority of voice streams in the voice VLAN.
Configuring the Voice VLAN Working Mode of a Port	(Optional) It is used to configure the voice VLAN working mode of a port.	
	voice vlan mode auto	Sets the voice VLAN working mode of a port to the automatic mode.

5.4.1 Enabling the Voice VLAN Function

Configuration Effect

- Configure a VLAN as the voice VLAN to transmit voice streams.

Notes

- Create a VLAN before configuring the voice VLAN.
- VLAN 1 is the default VLAN and does not need to be created, but VLAN 1 cannot be configured as the voice VLAN.
- A VLAN cannot be configured both as the voice VLAN and super VLAN.
- If 802.1x authentication with VLAN assignment is enabled on the port, do not configure the issued VLAN ID as the voice VLAN ID; otherwise, the function of 802.1x authentication with VLAN assignment is negatively affected.
- Do not configure the same VLAN as the remote VLAN and voice VLAN of the remote switched port analyzer (RSPAN); otherwise the RSPAN and voice VLAN functions may be negatively affected.

Configuration Steps

Configuring a Voice VLAN

- Mandatory.
- Create a VLAN, and configure this VLAN as the voice VLAN for transmission of voice streams.
- Perform this configuration on a switch.

Command	**voice vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates the ID of a VLAN. The value ranges from 2 to 4,094.
Defaults	By default, the voice VLAN function is disabled.
Command	Global configuration mode

Mode	
Usage Guide	Run the **no voice vlan** command in global configuration mode to disable the voice VLAN function.

Assume that both the 802.1x and voice VLAN functions are enabled on a port. If the device MAC address of an IP phone matches the OUI of the voice VLAN configured on the device, the IP phone can use the voice VLAN for communication without being authenticated. For example, if a PC and an IP phone are connected to the same port, and the 802.1x function is enabled, the PC must pass the 802.1x authentication before using the network for communication, but the IP phone does not need to be authenticated.

Verification

- Run the **show voice vlan** command to check whether the configuration takes effect.

Command	**show voice vlan**
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE --- ---

Configuration Example

Configuring a Voice VLAN

Configuration Steps	• Create VLAN 2. • Globally enable the voice VLAN function, and configure VLAN 2 as a voice VLAN.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# vlan 2

	Hostname(config-vlan)# exit Hostname(config)# voice vlan 2
Verification	Run the **show voice vlan** command to check whether the configuration is correct.
	Hostname#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 : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE --- ---

5.4.2 Enabling the Voice VLAN Function on a Port

Configuration Effect

Enable the voice VLAN function of a port connected to an IP phone. This step is mandatory to enable a port to transmit voice streams.

Notes

- The voice VLAN function can be enabled only on a Layer-2 (L2) port, such as the access port, trunk port, hybrid port, uplink port, and private VLAN port. It cannot be enabled on an AP port or a routed port.
- After the voice VLAN function is enabled on a port, to ensure normal operation of the function, do not switch the L2 mode (such as the access port, trunk port, and hybrid port) of the port. If L2 mode switching of a port is necessary, disable the voice VLAN port on this port first.

Configuration Steps

↘ **Enabling the Voice VLAN Function on a Port**

- Mandatory.
- You must enable the voice VLAN function on a port if you want to use this port for IP phone communication.
- Perform this configuration on a switch.

Command	**voice vlan enable**
Parameter De	N/A

scription	
Defaults	By default, the voice VLAN function is disabled on a port.
Command Mode	Interface configuration mode
Usage Guide	Run the **no voice vlan enable** command to disable the voice VLAN function on a port.

When the voice VLAN function is globally disabled, you can enable the voice VLAN function on a port, but this configuration does not take effect.

Verification

- Run the **show voice vlan** command to check whether the configuration takes effect.

Command	**show voice vlan**
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE ---------- ---------- Gi0/1 MANUAL

Configuration Example

Enabling the Voice VLAN Function on a Port

Configuration Steps	• Enter the port configuration mode, and enable the voice VLAN function on a physical port.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if)# voice vlan enable
Verification	Run the **show voice vlan** command to check whether the configuration is correct.
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE ---------- ---------- Gi0/1 MANUAL

5.4.3 Configuring the Aging Time of the Voice VLAN

Configuration Effect

- Configure the aging time of the voice VLAN on a device. If the device does not receive any voice packet from the input port within the aging time, the port is automatically deleted from the voice VLAN. The aging time takes effect only in automatic mode.

Configuration Steps

↘ **Configuring the Aging Time of the Voice VLAN**

- Optional.
- Perform this configuration if you need to change the time that a port resides in the voice VLAN before the port receives any voice stream.
- Perform this configuration on a switch.

Command	**voice vlan aging** *minutes*
Parameter Description	***minute :*** Indicates the aging time of the voice VLAN.
Defaults	By default, the aging time is 1,440 minutes.
Command	Global configuration mode

Mode	
Usage Guide	Run the **no voice vlan aging** command in global configuration mode to restore the default aging time.

Verification

- Run the **show voice vlan** command to check whether the configuration takes effect.

Command	**show voice vlan**
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE ---------- ----------

Configuration Example

Configuring the Aging Time of the Voice VLAN

Configuration Steps	• Set the aging time of the voice VLAN to 10 minutes.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# voice vlan aging 10
Verification	Run the **show voice vlan** command to check whether the configuration is correct.
	Hostname#show voice vlan Voice VLAN status : ENABLE

```
Voice VLAN ID           : 10

Voice VLAN security mode: Security

Voice VLAN aging time   : 10 minutes

Voice VLAN cos          : 6

Voice VLAN dscp         : 46

Current voice VLAN enabled port mode:

PORT                MODE

------------------- ----------
```

5.4.4 Configuring the OUI of the Voice VLAN

Configuration Effect

- Products support configuration of the OUI of a voice VLAN that can be identified. For details about the OUI, see "Overview". A device supporting the voice VLAN function can compare the source MAC address contained in a received packet with the OUI of the voice VLAN configured on the device to check whether the stream is a voice stream sent from a specified voice device.

Notes

- The OUI of the voice VLAN cannot be a multicast address, and the configured mask must be continuous.

Configuration Steps

↘ **Configuring the OUI of the Voice VLAN**

- Optional.
- After an IP phone is connected to the device that supports the voice VLAN, you need to configure the OUI of the IP phone so that the IP phone can implement communication on the network.
- Perform this configuration on a switch.

Command	**voice vlan mac-address** *mac-addr* **mask** *oui-mask* [**description** *text*]
Parameter Description	*mac-addr*: Indicates the source MAC address in a voice packet. *oui-mask*: Indicates the valid length of the OUI, which is expressed by a mask. ***text:*** Indicates the description about the OUI.
Defaults	By default, no OUI is configured.
Command Mode	Global configuration mode
Usage Guide	Run the **no voice vlan mac-address oui** command in global configuration mode to delete an OUI configured on a device.

Verification

- Run the **show voice vlan oui** command to check whether the configuration takes effect.

Command	**show voice vlan oui**
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname(config)# show voice vlan oui Oui Address Mask Description 0012.3400.0000 ffff.ff00.0000 Company A

Configuration Example

Configuring the OUI of the Voice VLAN

Configuration Steps	● Set the OUI of the voice VLAN to 0012.3400.0000, and the supplier is Company A.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A
Verification	Run the **show voice vlan oui** command to check whether the configuration is correct.
	Hostname(config)# show voice vlan oui Oui Address Mask Description 0012.3400.0000 ffff.ff00.0000 Company A

5.4.5 Configuring the Security Mode of the Voice VLAN

Configuration Effect

- To better isolate voice streams from data streams during transmission, the products support the security mode of the voice VLAN. When the security mode is enabled, only voice streams can be transmitted in the voice VLAN, which better ensures the quality of voice stream transmission.

Configuration Steps

Configuring the Security Mode of the Voice VLAN

- Optional.
- The security mode of the voice VLAN is configured to isolate voice streams from data streams. Perform this configuration if only voice streams can be transmitted in the voice VLAN.

- Perform this configuration on a switch.

Command	**voice vlan security enable**
Parameter Description	N/A
Defaults	By default, the security mode of the voice VLAN is enabled.
Command Mode	Global configuration mode
Usage Guide	Run the **no voice vlan security enable** command in global configuration mode to disable the security mode of the voice VLAN.

Verification

- Run the **show voice vlan** command to check whether the configuration takes effect.

Command	**show voice vlan**
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE ---------- ----------

Configuration Example

Configuring the Security Mode of the Voice VLAN

Configuration Steps	- Enter the global configuration mode, and enable the security mode of the voice VLAN.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# voice vlan security enable

Verification	Run the **show voice vlan** command to check whether the configuration is correct.
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE --- ---

5.4.6 Configuring the Priority of Voice Streams in the Voice VLAN

Configuration Effect

- Modify the CoS and DSCP values of voice streams in the voice VLAN to improve the priority of voice streams and ensure the quality of calls. For details about the CoS and DSCP, see "Configuring the QoS".

Configuration Steps

Configuring the Priority of Voice Streams in the Voice VLAN

- Optional.
- Perform this configuration if you need to improve the priority of voice streams.
- Perform this configuration on a switch.

Command	**voice vlan cos** *cos-value* **voice vlan dscp** *dscp-value*
Parameter Description	*cos-value:* Indicates the CoS value of voice streams in the voice VLAN. The value ranges from 0 to 7. *dscp-value:* Indicates the DSCP value of voice streams in the voice VLAN. The value ranges from 0 to 63.
Defaults	By default, the CoS is **6** and DSCP is **46**.
Command Mode	Global configuration mode
Usage Guide	Run the **no voice vlan cos** command to restore the default CoS value, or the **no voice vlan dscp** command to restore the default DSCP value.

Verification

- Run the **show voice vlan** command to check whether the configuration takes effect.

Command	**show voice vlan**
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE ---------- ----------

Configuration Example

Configuring the Priority of Voice Streams in the Voice VLAN

Configuration Steps	● Set the CoS of voice streams in the voice VLAN to **5** and the DSCP to **40**.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# voice vlan cos 5 Hostname(config)# voice vlan dscp 40
Verification	Run the **show voice vlan** command to check whether the configuration is correct.
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 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 ---------- ----------

5.4.7 Configuring the Voice VLAN Working Mode of a Port

Configuration Effect

- The voice VLAN may work in either automatic or manual mode. The working mode of the voice VLAN is configured in port configuration mode. For details about the automatic and manual modes, see "Automatic and Manual Modes of the Voice VLAN".

Notes

- If the voice VLAN function is enabled on a port and the voice VLAN works in manual mode, you must manually add the port to the voice VLAN to ensure that the voice VLAN function can take effect.
- When the voice VLAN function is enabled on a port and the voice VLAN works in automatic mode, do not configure the native VLAN of the port as the voice VLAN; otherwise, the voice VLAN function may be negatively affected.
- By default, the trunk or hybrid port of the product can transmit packets of all VLANs. You need to delete the voice VLAN from the allowed VLAN list of a port and then enable the voice VLAN function. In this way, ports that are not connected to any voice device will not be added to the voice VLAN, and ports that are not in use for a long time always reside in the voice VLAN.

Configuration Steps

Setting the Voice VLAN Working Mode of a Port to the Automatic Mode

- Optional.
- Perform this configuration if you want a port to be automatically added to the voice VLAN when the port receive voice streams and automatically deleted from the voice VLAN when the aging time expires.
- Perform this configuration on a switch.

Command	**voice vlan mode auto**
Parameter Description	N/A
Defaults	By default, the voice VLAN of a port works in automatic mode.
Command Mode	Interface configuration mode
Usage Guide	Run the **no voice vlan mode auto** command to set the voice VLAN working mode of a port to the manual mode.

After the voice VLAN function is enabled on a port, the working mode of the voice VLAN cannot be changed. To change the working mode of the voice VLAN, you must first disable the voice VLAN function on the port.

In automatic mode, you cannot use the manual configuration command (**switchport trunk allow vlan add**) to add a port to or delete a port from the voice VLAN.

Verification

- Run the **show voice vlan** command to check whether the configuration takes effect.

Command	show voice vlan
Parameter Description	N/A
Command Mode	All configuration modes
Usage Guide	N/A
	Hostname#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Voice VLAN cos : 6 Voice VLAN dscp : 46 Current voice VLAN enabled port mode: PORT MODE ---------- ---------- Gi0/1 AUTO

Configuration Example

Adding a Port to the Voice VLAN That Works in Automatic Mode

Scenario **Figure 5-4**	
Configuration Steps	Configuration Tips ● The Fa 0/1 port is connected to an IP phone that automatically obtains the IP address. After obtaining the IP address in the voice VLAN, the IP phone can be used normally. The Fa 0/1 port is required to forward both voice and data streams and isolate voice streams from data streams. The port can be configured as a trunk port. The native VLAN forwards data streams, whereas the voice VLAN forwards voice streams. ● The PC sends untagged packets. Therefore, the packets will be transmitted in the native VLAN of the port. Configure VLAN 5 as the native VLAN to transmit data streams sent by the PC. ● The network is required to isolate voice streams from data streams. When the port is configured as a trunk port, and the automatic mode is configured as the working mode of the voice VLAN, the native VLAN of the Fa0/1 port must exist and cannot be a voice VLAN according to the matching relationship. In addition, the port must allow packets of the native VLAN to pass through. The ID of the native VLAN is 5, and the native VLAN is not a voice VLAN (VLAN 2). Therefore, the networking requirement for isolating voice streams from data streams can be met. As the trunk port contains all VLANs by default, to better use the automatic mode and prevent ports that are not connected with any voice device from being added to the voice VLAN, the voice VLAN (VLAN 2) must be deleted from the allowed VLAN list of the Fa0/1 port.

	Step 1: Create VLAN 2, and configure this VLAN as the voice VLAN.
	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# vlan 2`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# voice vlan 2`
	
	Step 2: Configure data on the device so that the device allows voice packets with the OUI set to 0012.3400.0000 and mask set to ffff.ff00.0000 to be forwarded through the voice VLAN.

	Hostname(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 Step 3: Configure Fa0/1 as the trunk port, and VLAN 5 as the native VLAN of the port. Hostname(config)# interface fastEthernet 0/1 Hostname(config-if)# switchport mode trunk Hostname(config-if)# switchport trunk native vlan 5 Step 4: Delete the voice VLAN from the allowed VLAN list of the Fa0/1 port, and enable the voice VLAN function of the Fa0/1 port. Hostname(config-if)# switchport trunk allowed vlan remove 2 Hostname(config-if)# voice vlan enable
Verification	● Run the **show voice vlan** command to check the current status of the voice VLAN on the device.
	Hostname(config)# 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 : 6 Voice Vlan dscp : 46 Current voice vlan enabled port mode: PORT MODE ---------- ---------- Fa0/1 AUTO # Check Voice VLAN OUI Address Hostname(config)# show voice vlan oui Oui Address Mask Description 0012.3400.0000 ffff.ff00.0000

5.5 Monitoring

Displaying

Description	Command
Displays the voice VLAN configuration.	**show voice vlan**
Displays the OUI configuration of the voice VLAN.	**show voice vlan oui**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the voice VLAN.	**debug bridge vvlan**

6 Configuring MSTP

6.1 Overview

Spanning Tree Protocol (STP) is a Layer-2 management protocol. It cannot only selectively block redundant links to eliminate Layer-2 loops but also can back up links.

Similar to many protocols, STP is continuously updated from Rapid Spanning Tree Protocol (RSTP) to Multiple Spanning Tree Protocol (MSTP) as the network develops.

For the Layer-2 Ethernet, only one active link can exist between two local area networks (LANs). Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

RSTP is completely compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

STP and RSTP have the following defects:

- STP migration is slow. Even on point-to-point links or edge ports, it still takes two times of the forward delay for ports to switch to the forwarding state.
- RSTP can rapidly converge but has the same defect with STP: Since all VLANs in a LAN share the same spanning tree, packets of all VLANs are forwarded along this spanning tree. Therefore, redundant links cannot be blocked according to specific VLANs and data traffic cannot be balanced among VLANs.

MSTP, defined by the IEEE in 802.1s, resolves defects of STP and RSTP. It cannot only rapidly converge but also can enable traffic of different VLANs to be forwarded along respective paths, thereby providing a better load balancing mechanism for redundant links.

In general, STP/RSTP works based on ports while MSTP works based on instances. An instance is a set of multiple VLANs. Binding multiple VLANs to one instance can reduce the communication overhead and resource utilization.

Devices support STP, RSTP, and MSTP, and comply with IEEE 802.1D, IEEE 802.1w, and IEEE 802.1s.

Protocols and Standards

- IEEE 802.1D: Media Access Control (MAC) Bridges
- IEEE 802.1w: Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s: Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

6.2 Applications

Application	Description
MSTP+VRRP Dual-Core Topology	With a hierarchical network architecture model, the MSTP+VRRP mode is used to implement redundancy and load balancing to improve system availability of the network.
BPDU Tunnel	In QinQ network environment, Bridge Protocol Data Unit (BPDU) Tunnel is used to implement tunnel-based transparent transmission of STP packets.

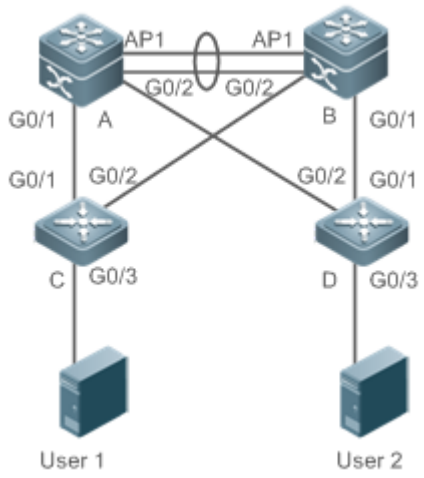
6.2.1 MSTP+VRRP Dual-Core Topology

Scenario

The typical application of MSTP is the MSTP+VRRP dual-core solution. This solution is an excellent solution to improve system availability of the network. Using a hierarchical network architecture model, it is generally divided into three layers (core layer, convergence layer, and access layer) or two layers (core layer and access layer). They form the core network system to provide data exchange service.

The main advantage of this architecture is its hierarchical structure. In the hierarchical network architecture, all capacity indicators, characteristics, and functions of network devices at each layer are optimized based on their network locations and roles, enhancing their stability and availability.

Figure 6-1 MSTP+VRRP Dual-Core Topology



Remarks	The topology is divided into two layers: core layer (Devices A and B) and access layer (Devices C and D).

Deployment

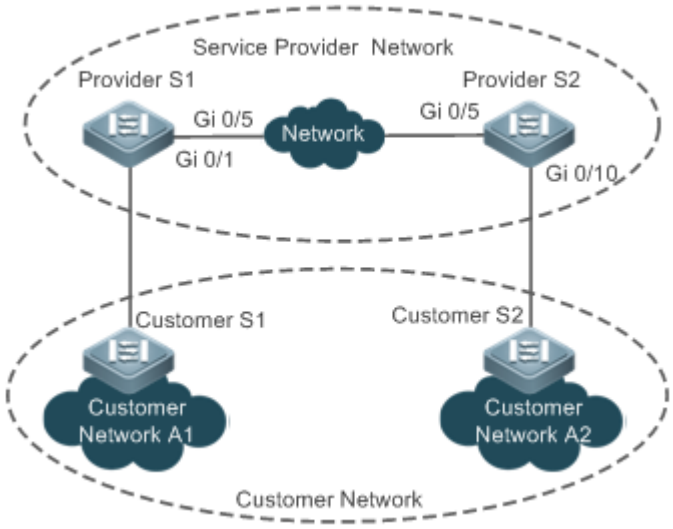
- Core layer: Multiple MSTP instances are configured to realize load balancing. For example, two instances are created: Instance 1 and Instance 2. Instance 1 maps VLAN 10 while Instance 2 maps VLAN 20. Device A is the root bridge of Instances 0 and 1 (Instance 0 is CIST, which exists by default). Device B is the root bridge of Instance 2.
- Core layer: Devices A and B are the active VRRP devices respectively on VLAN 10 and VLAN 20.
- Access layer: Configure the port directly connected to the terminal (PC or server) as a PortFast port, and enable BPDU guard to prevent unauthorized users from accessing illegal devices.

6.2.2 BPDU Tunnel

Scenario

The QinQ network is generally divided into two parts: customer network and service provider (SP) network. You can enable BPDU Tunnel to calculate STP packets of the customer network independently of the SP network, thereby preventing STP packets between the customer network from affecting the SP network.

Figure 6-2 BPDU Tunnel Topology



Remarks	As shown in the above figure, the upper part is the SP network and the lower part is the customer network. The SP network consists of two provider edges (PEs): Provider S1 and Provider S2. Customer Network A1 and Customer Network A2 are a user's two sites in different regions. Customer S1 and Customer S2, access devices from the customer network to the SP network, access the SP network respectively through Provider S1 and Provider S2. Using BPDU Tunnel, Customer Network A1 and Customer Network A2 in different regions can perform unified spanning tree calculation across the SP network, not affecting the spanning tree calculation of the SP network.

Deployment

- Enable basic QinQ on the PEs (Provider S1/Provider S2 in this example) so that data packets of the customer network are transmitted within the specified VLAN on the SP network.
- Enable STP transparent transmission on the PEs (Provider S1/Provider S2 in this example) so that the SP network can transmit STP packets of the customer network through BPDU Tunnel.

6.3 Features

Basic Concepts

BPDU

To generate a stable tree topology network, the following conditions must be met:

- Each bridge has a unique ID consisting of the bridge priority and MAC address.
- The overhead of the path from the bridge to the root bridge is called root path cost.
- A port ID consists of the port priority and port number.

Bridges exchange BPDU packets to obtain information required for establishing the best tree topology. These packets use the multicast address 01-80-C2-00-00-00 (hexadecimal) as the destination address.

A BPDU consists of the following elements:

- Root bridge ID assumed by the local bridge
- Root path cost of the local bridge
- Bridge ID (ID of the local bridge)
- Message age (age of a packet)
- Port ID (ID of the port sending this packet)
- **Forward-Delay Time**, **Hello Time**, **Max-Age Time** are time parameters specified in the MSTP.
- Other flags, such as flags indicating network topology changes and local port status.

If a bridge receives a BPDU with a higher priority (smaller bridge ID and lower root path cost) at a port, it saves the BPDU information at this port and transmits the information to all other ports. If the bridge receives a BPDU with a lower priority, it discards the information.

Such a mechanism allows information with higher priorities to be transmitted across the entire network. BPDU exchange results are as follows:

- A bridge is selected as the root bridge.
- Except the root bridge, each bridge has a root port, that is, a port providing the shortest path to the root bridge.
- Each bridge calculates the shortest path to the root bridge.
- Each LAN has a designated bridge located in the shortest path between the LAN and the root bridge. A port designated to connect the bridge and the LAN is called designated port.
- The root port and designated port enter the forwarding status.

Bridge ID

According to IEEE 802.1W, each bridge has a unique ID. The spanning tree algorithm selects the root bridge based on the bridge ID. The bridge ID consists of eight bytes, of which the last six bytes are the MAC address of the bridge. In its first two bytes (as listed in the following table), the first four bits indicate the priority; the last eight bits indicate the system ID for use in extended protocol. In RSTP, the system ID is 0. Therefore, the bridge priority should be an integral multiple of 4,096.

	Bit	Value
Priority value	16	32,768
	15	16,384
	14	8,192
	13	4,096
System ID	12	2,048
	11	1,024
	10	512
	9	256
	8	128
	7	64
	6	32
	5	16
	4	8
	3	4
	2	2
	1	1

Spanning-Tree Timers

The following three timers affect the performance of the entire spanning tree:

- Hello timer: Interval for periodically sending a BPDU packet.
- Forward-Delay timer: Interval for changing the port status, that is, interval for a port to change from the listening state to the learning state or from the learning state to the forwarding state when RSTP runs in STP-compatible mode.
- Max-Age timer: The longest time-to-live (TTL) of a BPDU packet. When this timer elapses, the packet is discarded.

Port Roles and Port States

Each port plays a role on a network to reflect different functions in the network topology.

- Root port: Port providing the shortest path to the root bridge.
- Designated port: Port used by each LAN to connect the root bridge.
- Alternate port: Alternative port of the root port. Once the root port loses effect, the alternate port immediately changes to the root port.
- Backup port: Backup port of the designated port. When a bridge has two ports connected to a LAN, the port with the higher priority is the designated port while the port with the lower priority is the backup port.

- Disabled port: Inactive port. All ports with the operation state being down play this role.

The following figures show the roles of different ports:

R = Root port D = Designated port A = Alternate port B = Backup port

Unless otherwise specified, port priorities decrease from left to right.

Figure 6-3

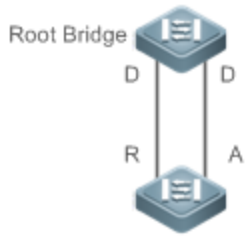


Figure 6-4

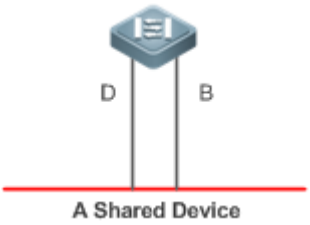
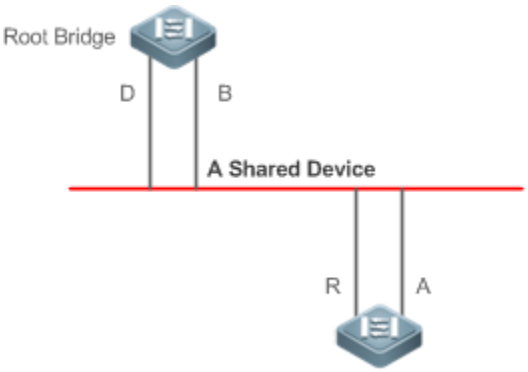


Figure 6-5



Each port has three states indicating whether to forward data packets so as to control the entire spanning tree topology.

- Discarding: Neither forwards received packets nor learns the source MAC address.
- Learning: Does not forward received packets but learns the source MAC address, which is a transitive state.
- Forwarding: Forwards received packets and learns the source MAC address.

For a stable network topology, only the root port and designated port can enter the forwarding state while other ports are always in discarding state.

Hop Count

Internal spanning trees (ISTs) and multiple spanning tree instances (MSTIs) calculate whether the BPDU packet time expires based on an IP TTL-alike mechanism Hop Count, instead of Message Age and Max Age.

It is recommended to run the **spanning-tree max-hops** command in global configuration mode to configure the hop count. In a region, every time a BPDU packet passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU packet time expires and the device discards the packet.

To be compatible with STP and RSTP outside the region, MSTP also retains the Message Age and Max Age mechanisms.

Overview

Feature	Description
STP	STP, defined by the IEEE in 802.1D, is used to eliminate physical loops at the data link layer in a LAN.
RSTP	RSTP, defined by the IEEE in 802.1w, is optimized based on STP to rapidly converge the network topology.
MSTP	MSTP, defined by the IEEE in 802.1s, resolves defects of STP, RSTP, and Per-VLAN Spanning Tree (PVST). It cannot only rapidly converge but also can forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.
MSTP Optical Features	MSTP includes the following features: PortFast, BPDU guard, BPDU filter, TC protection, TC guard, TC filter, BPDU check based on the source MAC address, BPDU filter based on the illegal length, Auto Edge, root guard, and loop guard.

6.3.1 STP

STP is used to prevent broadcast storms incurred by loops and provide link redundancy.

Working Principle

For the Layer-2 Ethernet, only one active link can exist between two LANs. Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

6.3.2 RSTP

RSTP is completely compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the

administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

Working Principle

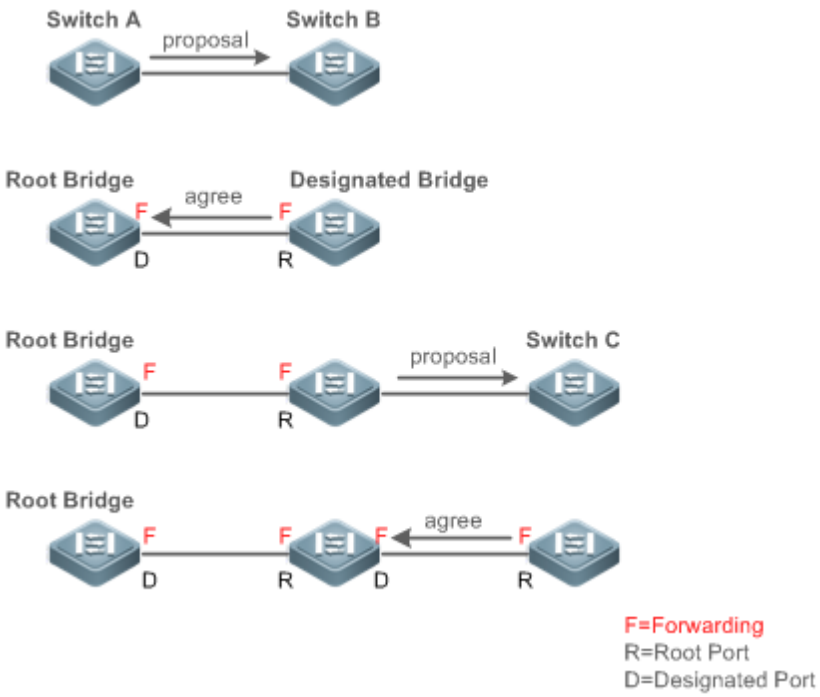
Fast RSTP Convergence

RSTP has a special feature, that is, to make ports quickly enter the forwarding state.

STP enables a port to enter the forwarding state 30 seconds (two times of the Forward-Delay Time; the Forward-Delay Time can be configured, with a default value of 15 seconds) after selecting a port role. Every time the topology changes, the root port and designated port reselected by each bridge enter the forwarding state 30 seconds later. Therefore, it takes about 50 seconds for the entire network topology to become a tree.

RSTP differs greatly from STP in the forwarding process. As shown in Figure 6-6, Switch A sends an RSTP Proposal packet to Switch B. If Switch B finds the priority of Switch A higher, it selects Switch A as the root bridge and the port receiving the packet as the root port, enters the forwarding state, and then sends an Agree packet from the root port to Switch A. If the designated port of Switch A is agreed, the port enters the forwarding state. Switch B's designated port resends a Proposal packet to extend the spanning tree by sequence. Theoretically, RSTP can recover the network tree topology to rapidly converge once the network topology changes.

Figure 6-6



The above handshake process is implemented only when the connection between ports is in point-to-point mode. To give the devices their full play, it is recommended not to enable point-to-point connection between devices.

Figure 6-7 and Figure 6-8 show the examples of non-point-to-point connection.

Example of non-point-to-point connection:

Figure 6-7

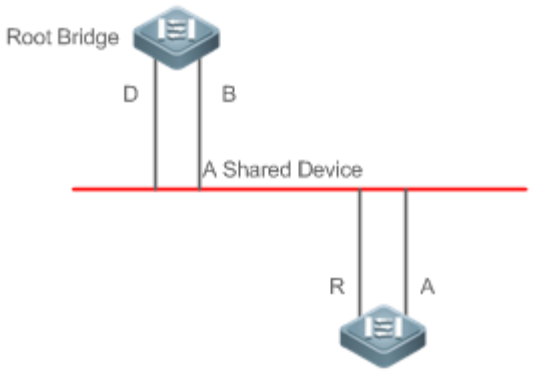


Figure 6-8

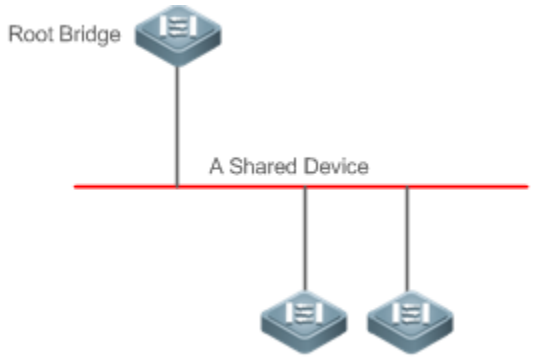
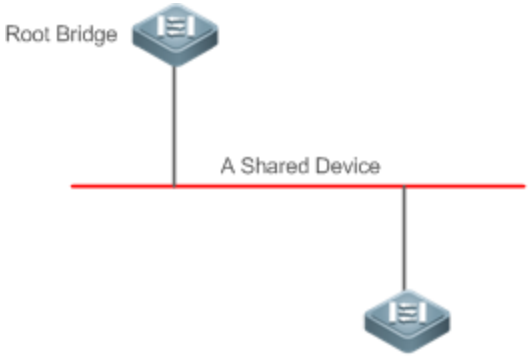


Figure 6-9 shows an example of point-to-point connection.

Figure 6-9



Compatibility Between RSTP and STP

RSTP is completely compatible with STP. RSTP automatically checks whether the connected bridge supports STP or RSTP based on the received BPDU version number. If the port connects to an STP bridge, the port enters the forwarding state 30 seconds later, which cannot give RSTP its full play.

Another problem may occur when RSTP and STP are used together. As shown in the following figures, Switch A (RSTP) connects to Switch B (STP). If Switch A finds itself connected to an STP bridge, it sends an STP BPDU packet. However, if Switch B is replaced with Switch C (RSTP) but Switch A still sends STP BPDU packets, Switch C will assume itself connected to the STP bridge. As a result, two RSTP devices work under STP, greatly reducing the efficiency.

RSTP provides the protocol migration feature to forcibly send RSTP BPDU packets (the peer bridge must support RSTP). In this case, Switch A is enforced to send an RSTP BPDU and Switch C then finds itself connected to the RSTP bridge. As a result, two RSTP devices work under RSTP, as shown in Figure 6-11.

Figure 6-10

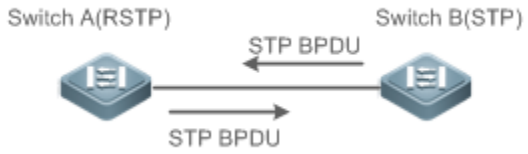
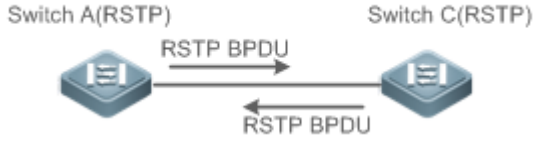


Figure 6-11



6.3.3 MSTP

MSTP resolves defects of STP and RSTP. It cannot only rapidly converge but also can forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.

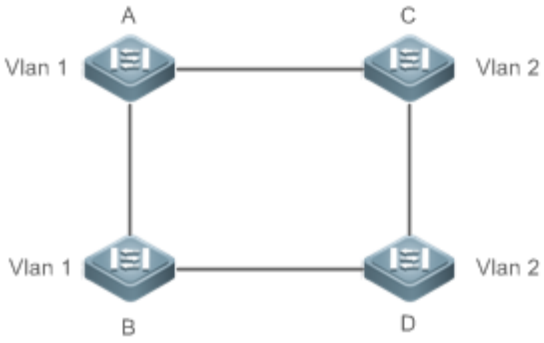
Working Principle

Devices support MSTP. MSTP is a new spanning tree protocol developed from traditional STP and RSTP and includes the fast RSTP forwarding mechanism.

Since traditional spanning tree protocols are irrelevant to VLANs, problems may occur in specific network topologies:

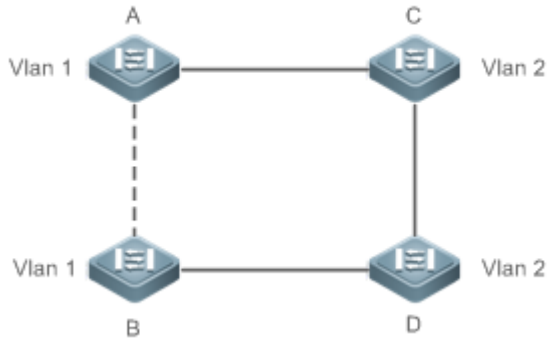
As shown in Figure 6-12, Devices A and B are in VLAN 1 while Devices C and D are in VLAN 2, forming a loop.

Figure 6-12



If the link from Device A to Device B through Devices C and D costs less than the link from Device A direct to Device B, the link between Device A and Device B enters the discarding state (as shown in Figure 6-13). Since Devices C and D do not include VLAN 1 and cannot forward data packets of VLAN 1, VLAN 1 of Device A fails to communicate with VLAN 1 of Device B.

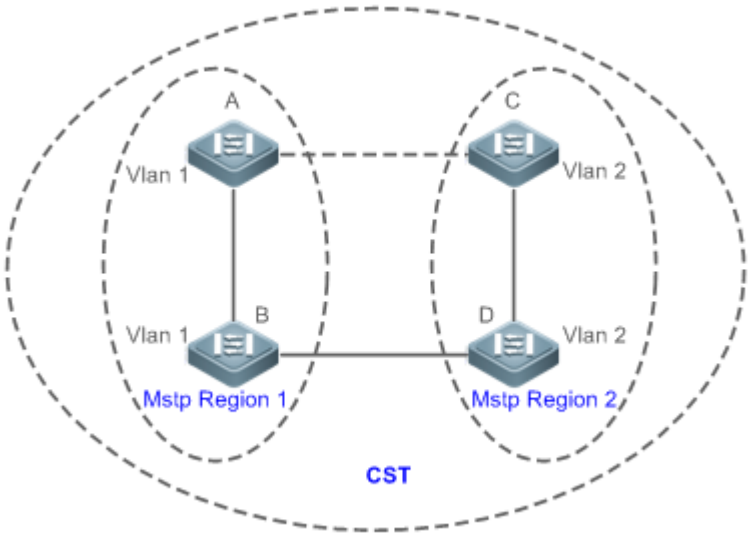
Figure 6-13



MSTP is developed to resolve this problem. It divides one or multiple VLANs of a device into an instance. Devices configured with the same instance form an MST region to run an independent spanning tree (called IST). This MST region, like a big device, implements the spanning tree algorithm with other MST regions to generate a complete spanning tree called common spanning tree (CST).

Based on this algorithm, the above network can form the topology shown in Figure 6-14 under the MSTP algorithm: Devices A and B are in MSTP region 1 in which no loop occurs, and therefore no link enters the discarding state. This also applies to MSTP Region 2. Region 1 and Region 2, like two big devices having loops, select a link to enter the discarding state based on related configuration.

Figure 6-14



This prevents loops to ensure proper communication between devices in the same VLAN.

MSTP Region Division

To give MSTP its due play, properly divide MSTP regions and configure the same MST configuration information for devices in the same MSTP region.

MST configuration information include:

- MST configuration name: Consists of at most 32 bytes to identify an MSTP region.
- MST Revision Number: Consists of 16 bits to identify an MSTP region.
- MST instance-VLAN mapping table: A maximum number of 64 instances (with their IDs ranging from 1 to 64) are created for each device and Instance 0 exists mandatorily. Therefore, the system supports a maximum number of 65 instances. Users can assign 1 to 4,994 VLANs belonging to different instances (ranging from 0 to 64) as required. Unassigned VLANs belong to Instance 0 by default. In this case, each MSTI is a VLAN group and implements the spanning tree algorithm of the MSTI specified in the BPDU packet, not affected by CIST and other MSTIs.

Run the **spanning-tree mst configuration** command in global configuration mode to enter the MST configuration mode to configure the above information.

MSTP BPDUs carry the above information. If the BPDU received by a device carries the same MST configuration information with the information on the device, it regards that the connected device belongs to the same MST region with itself. Otherwise, it regards the connected device originated from another MST region.

It is recommended to configure the instance-VLAN mapping table after disabling MSTP. After the configuration, re-enable MSTP to ensure stability and convergence of the network topology.

IST (Spanning Tree in an MSTP Region)

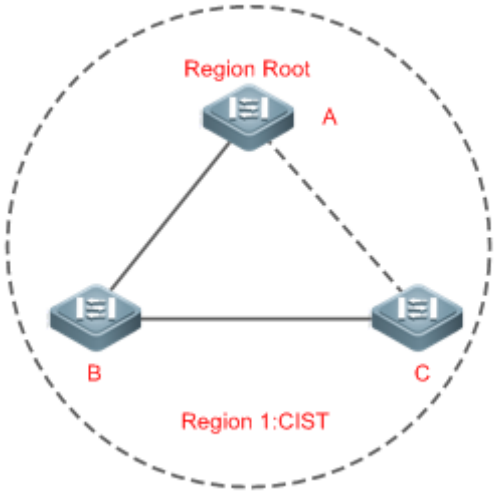
After MSTP regions are divided, each region selects an independent root bridge for each instance based on the corresponding parameters such as bridge priority and port priority, assigns roles to each port on each device, and specifies whether the port is in forwarding or discarding state in the instance based on the port role.

Through MSTP BPDU exchange, an IST is generated and each instance has their own spanning trees (MSTIs), in which the spanning tree corresponding to Instance 0 and CST are uniformly called Common Instance Spanning Tree (CIST). That is, each instance provides a single and loop-free network topology for their own VLAN groups.

As shown in Figure 6-15, Devices A, B, and C form a loop in Region 1.

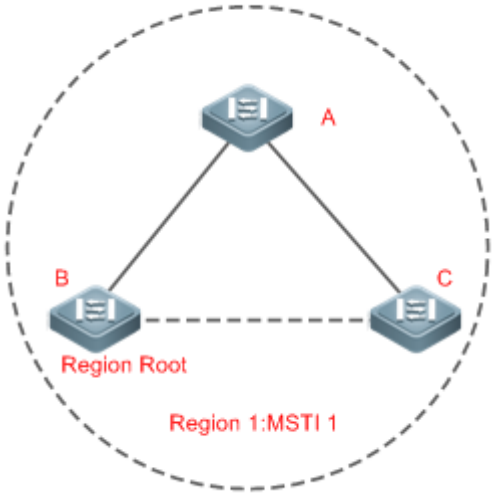
As shown in Figure 6-15, Device A has the highest priority in the CIST (Instance 0) and thereby is selected as the region root. Then MSTP enables the link between A and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 0, only links from A to B and from B to C are available, interrupting the loop of this VLAN group.

Figure 6-15



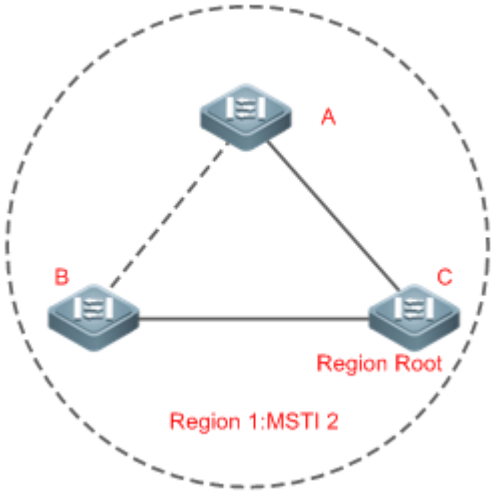
As shown in Figure 6-16, Device B has the highest priority in the MSTI 1 (Instance 1) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 1, only links from A to B and from A to C are available, interrupting the loop of this VLAN group.

Figure 6-16



As shown in Figure 6-17, Device C has the highest priority in the MSTI 2 (Instance 2) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 2, only links from B to C and from A to C are available, interrupting the loop of this VLAN group.

Figure 6-17

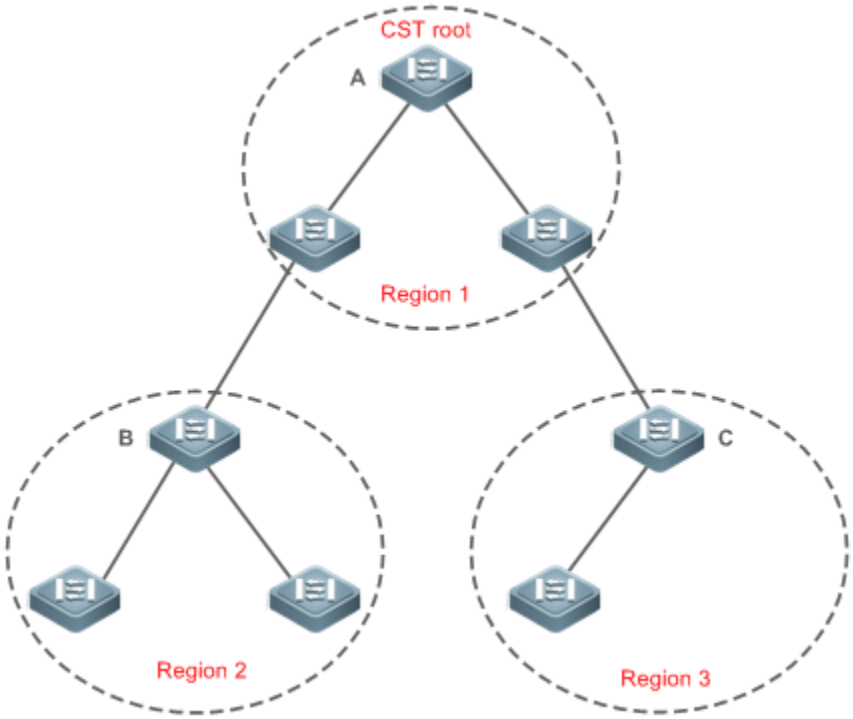


Note that MSTP does not care which VLAN a port belongs to. Therefore, users should configure the path cost and priority of a related port based on the actual VLAN configuration to prevent MSTP from interrupting wrong loops.

CST (Spanning Tree Between MSTP Regions)

Each MSTP region is like a big device for the CST. Different MSTP regions form a bit network topology tree called CST. As shown in Figure 6-18, Device A, of which the bridge ID is the smallest, is selected as the root in the entire CST and the CIST regional root in this region. In Region 2, since the root path cost from Device B to the CST root is lowest, Device B is selected as the CIST regional root in this region. For the same reason, Device C is selected as the CIST regional root.

Figure 6-18



The CIST regional root may not be the device of which the bridge ID is the smallest in the region but indicates the device of which the root path cost from this region to the CST root is the smallest.

For the MSTI, the root port of the CIST regional root has a new role "master port". The master port acts as the outbound port of all instances and is in forwarding state for all instances. To make the topology more stable, we suggest that the master port of each region to the CST root be on the same device of the region if possible.

Compatibility Among MSTP, RSTP, and STP

Similar to RSTP, MSTP sends STP BPDUs to be compatible with STP. For details, see "Compatibility Between RSTP and STP".

Since RSTP processes MSTP BPDUs of the CIST, MSTP does not need to send RSTP BPDUs to be compatible with it.

Each STP or RSTP device is a single region and does not form the same region with any devices.

6.3.4 MSTP Optional Features

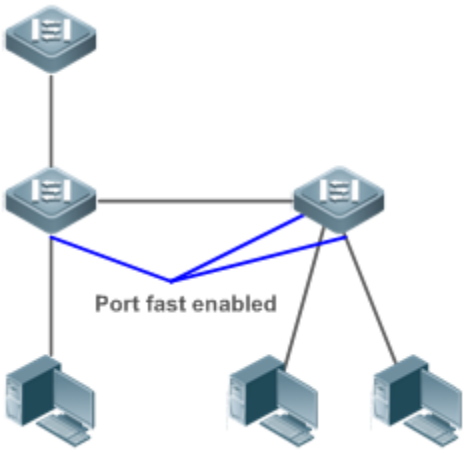
MSTP optional features mainly include PortFast port, BPDU guard, BPDU filter, TC guard, and guard. The optional features are mainly used to deploy MSTP configurations based on the network topology and application characteristics in the MSTP network. This enhances the stability, robustness, and anti-attack capability of MSTP, meeting application requirements of MSTP in different customer scenarios.

Working Principle

PortFast

If a port of a device connects directly to the network terminal, this port is configured as a PortFast port to directly enter the forwarding state. If the PortFast port is not configured, the port needs to wait for 30 seconds to enter the forwarding state. Figure 6-19 shows which ports of a device can be configured as PortFast ports.

Figure 6-19



If a PortFast port still receives BPDUs, its Port Fast Operational State is Disabled and the port enters the forwarding state according to the normal STP algorithm.

BPDU Guard

BPDU guard can be enabled globally or enabled on an interface.

It is recommended to run the **spanning-tree portfast bpduguard default** command in global configuration mode to enable global BPDU guard. If PortFast is enabled on a port or this port is automatically identified as an edge port, this port enters the error-disabled state to indicate the configuration error immediately after receiving a BPDU. At the same time, the port is disabled, indicating that a network device may be added by an unauthorized user to change the network topology.

It is also recommended to run the **spanning-tree bpduguard enable** command in interface configuration mode to enable BPDU guard on a port (whether PortFast is enabled or not on the port). In this case, the port enters the error-disabled state immediately after receiving a BPDU.

BPDU Filter

BPDU filter can be enabled globally or enabled on an interface.

It is recommended to run the **spanning-tree portfast bpdufilter default** command in global configuration mode to enable global BPDU filter. In this case, the PortFast port neither receives nor sends BPDUs and therefore the host connecting directly to the PortFast port receives no BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically loses effect.

It is also recommended to run the **spanning-tree bpdufilter enable** command in interface configuration mode to enable BPDU filter on a port (whether PortFast is enabled or not on the port). In this case, the port neither receives nor sends BPDUs but directly enters the forwarding state.

TC Protection

TC BPDUs are BPDU packets carrying the TC. If a switch receives such packets, it indicates the network topology changes and the switch will delete the MAC address table. For Layer-3 switches in this case, the forwarding module is re-enabled and the port status in the ARP entry changes. When a switch is attacked by forged TC BPDUs, it will frequently perform the above operations, causing heavy load and affecting network stability. To prevent this problem, you can enable TC protection.

TC protection can only be globally enabled or disabled. This function is disabled by default.

When TC protection is enabled, the switch deletes TC BPDUs within a specified period (generally 4 seconds) after receiving them and monitors whether any TC BPDU packet is received during the period. If a device receives TC BPDU packets during this period, it deletes them when the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries.

TC Guard

TC protection ensures less dynamic MAC addresses and ARP entries removed when a large number of TC packets are generated on the network. However, a device receiving TC attack packets still performs many removal operations and TC packets can be spread, affecting the entire network. Users can enable TC guard to prevent TC packets from spreading globally or on a port. If TC guard is enabled globally or on a port, a port receiving TC packets filters these TC packets or TC packets generated by itself so that TC packets will not be spread to other ports. This can effectively control possible TC attacks in the network to ensure network stability. Particularly on Layer-3 devices, this function can effectively prevent the access-layer device from flapping and interrupting the core route.

- If TC guard is used incorrectly, the communication between networks is interrupted.
- It is recommended to enable this function only when illegal TC attack packets are received in the network.
- If TC guard is enabled globally, no port spreads TC packets to others. This function can be enabled only on laptop access devices.
- If TC guard is enabled on a port, the topology changes incurred and TC packets received on the port will not be spread to other ports. This function can be enabled only on uplink ports, particularly on ports of the convergence core.

TC Filter

If TC guard is enabled on a port, the port does not forward TC packets received and generated by the port to other ports performing spanning tree calculation on the device. When the status of a port changes (for example, from blocking to forwarding), the port generates TC packets, indicating that the topology may have changed.

In this case, since TC guard prevents TC packets from spreading, the device may not clear the MAC addresses of the port when the network topology changes, causing a data forwarding error.

To resolve this problem, TC filter is introduced. TC filter does not process TC packets received by ports but processes TC packets in case of normal topology changes. If TC filter is enabled, the address removal problem will be avoided and the core route will not be interrupted when ports not enabled with PortFast frequently go up or down, and the core routing entries can be updated in a timely manner when the topology changes.

- TC filter is disabled by default.

BPDU Source MAC Address Check

BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address. If you run the **no bpdu src-mac-check** command to disable BPDU source MAC address check on a port, the port receives all BPDU packets.

BPDU Filter

If the Ethernet length of a BPDU exceeds 1,500, this BPDU will be discarded, preventing receipt of illegal BPDU packets.

Auto Edge

If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.

You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

This function is enabled by default.

- If Auto Edge conflicts with the manually configured PortFast, the manual configuration prevails.
- Since this function is used for rapid negotiation and forwarding between the designated port and the downlink port, STP does not support this function. If the designated port is in forwarding state, the Auto Edge configuration does not take effect on this port. It takes only when rapid negotiation is re-performed, for example, when the network cable is removed and plugged.
- If BPDU filter has been enabled on a port, the port directly enters the forwarding state and is not automatically identified as an edge port.
- This function applies only to the designated port.

Root Guard

In the network design, the root bridge and backup root bridge are usually divided into the same region. Due to incorrect configuration of maintenance personnel or malicious attacks in the network, the root bridge may receive configuration information with a higher priority and thereby switches to the backup root bridge, causing incorrect changes in the network topology. Root guard is to resolve this problem.

If root guard is enabled on a port, its roles on all instances are enforced as the designated port. Once the port receives configuration information with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive configuration information with a higher priority within a period, it returns to its original state.

If a port enters the blocking state due to root guard, you can manually restore the port to the normal state by disabling root guard on this port or disabling spanning tree guard (running **spanning-tree guard none** in interface configuration mode).

- If root guard is used incorrectly, the network link will be interrupted.
- If root guard is enabled on a non-designated port, this port will be enforced as a designated port and enter the BKN state. This indicates that the port enters the blocking state due to root inconsistency.

If a port enters the BKN state due to receipt of configuration information with a higher priority in MST0, this port will be enforced in the BKN state in all other instances.

Root guard and loop guard cannot take effect on a port at the same time.

Loop Guard

Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is to prevent this problem.

If a port enabled with loop guard does not receive BPDUs, the port switches its role but stays in discarding state till it receives BPDUs and recalculates the spanning tree.

You can enable loop guard globally or on a port.

Root guard and loop guard cannot take effect on a port at the same time.

Before MSTP is restarted on a port, the port enters the blocking state in loop guard. If the port still receives no BPDU after MSTP is restarted, the port will become a designated port and enter the forwarding state. Therefore, it is recommended to identify the cause why a port enters the blocking state in loop protection and rectify the fault as soon as possible before restarting MSTP. Otherwise, the spanning tree topology will still become abnormal after MSTP is restarted.

BPDU Transparent Transmission

In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliant with IEEE 802.1Q do not forward the BPDU packets received. However, devices may need to transparently transmit BPDU packets in actual network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated.

BPDU transparent transmission is disabled by default.

BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

BPDU Tunnel

The QinQ network is generally divided into two parts: customer network and SP network. Before a user packet enters the SP network, it is encapsulated with the VLAN tag of an SP network and also retains the original VLAN tag as data. As a result, the packet carries two VLAN tags to pass through the SP network. In the SP network, packets are transmitted only based on the outer-layer VLAN tag. When packets leave the SP network, the outer-layer VLAN tag is removed.

The STP packet transparent transmission feature, namely BPDU Tunnel, can be used to realize the transmission of STP packets between the customer network without any impact on the SP network. If an STP packet sent from the customer network enters a PE, the PE changes the destination MAC address of the packet to a private address before the packet is forwarded by the SP network. When the packet reaches the PE at the peer end, the PE changes the destination MAC address to a public address and returns the packet to the customer network at the peer end, realizing transparent transmission across the SP network. In this case, STP on the customer network is calculated independently of that on the SP network.

6.4 Configuration

Configuration	Description and Command	
Enabling STP	(Mandatory) It is used to enable STP.	
	spanning-tree	Enables STP and configures basic attributes.
	spanning-tree mode	Configures the STP mode.
Configuring STP Compatibility	(Optional) It is used to be compatible with competitor devices.	
	spanning-tree compatible enable	Enables the compatibility mode of a port.
	clear spanning-tree detected-protocols	Performs mandatory version check for BPDUs.
Configuring an MSTP Region	(Optional) It is used to configure an MSTP region.	
	spanning-tree mst configuration	Enters the MST configuration mode.
Enabling Fast RSTP Convergence	(Optional) It is used to configure whether the link type of a port is point-to-point connection.	
	spanning-tree link-type	Configures the link type.
Configuring Priorities	(Optional) It is used to configure the switch priority or port priority.	
	spanning-tree priority	Configures the switch priority.
	spanning-tree port-priority	Configures the port priority.
Configuring the Port Path Cost	(Optional) It is used to configure the path cost of a port or the default path cost calculation method.	
	spanning-tree cost	Configures the port path cost.
	spanning-tree pathcost method	Configures the default path cost calculation method.
Configuring the Maximum Hop Count of a BPDU Packet	(Optional) It is used to configure the maximum hop count of a BPDU packet.	
	spanning-tree max-hops	Configures the maximum hop count of a BPDU packet.
Enabling PortFast-related Features	(Optional) It is used to enable PortFast-related features.	
	spanning-tree portfast	Enables PortFast.
	spanning-tree portfast bpduguard default	Enables BPDU guard on all ports.
	spanning-tree bpduguard enabled	Enables BPDU guard on a port.
	spanning-tree portfast bpdufilter default	Enables BPDU filter on all ports.
	spanning-tree bpdufilter enabled	Enables BPDU filter on a port.

Configuration	Description and Command	
Enabling TC-related Features	(Optional) It is used to enable TC-related features.	
	spanning-tree tc-protection	Enables TC protection.
	spanning-tree tc-protection tc-guard	Enables TC guard on all ports.
	spanning-tree tc-guard	Enables TC guard on a port.
	spanning-tree ignore tc	Enables TC filter on a port.
Enabling BPDU Source MAC Address Check	(Optional) It is used to enable BPDU source MAC address check.	
	bpdu src-mac-check	Enables BPDU source MAC address check on a port.
Configuring Auto Edge	(Optional) It is used to configure Auto Edge.	
	spanning-tree autoedge	Enables Auto Edge on a port. This function is enabled by default.
Enabling Guard-related Features	(Optional) It is used to enable port guard features.	
	spanning-tree guard root	Enables root guard on a port.
	spanning-tree loopguard default	Enables loop guard on all ports.
	spanning-tree guard loop	Enables loop guard on a port.
	spanning-tree guard none	Disables the guard feature on a port.
Enabling BPDU Transparent Transmission	(Optional) It is used to enable BPDU transparent transmission	
	bridge-frame forwarding protocol bpdu	Enables BPDU transparent transmission.
Enabling BPDU Tunnel	(Optional) It is used to enable BPDU Tunnel.	
	l2protocol-tunnel stp	Enables BPDU Tunnel globally.
	l2protocol-tunnel stp enable	Enables BPDU Tunnel on a port.
	l2protocol-tunnel stp tunnel-dmac	Configures the transparent transmission address of BPDU Tunnel.

6.4.1 Enabling STP

Configuration Effect

- Enable STP globally and configure the basic attributes.
- Configure the STP mode.

Notes

- STP is disabled by default. Once STP is enabled, the device starts to run STP. The device runs MSTP by default.
- The default STP mode is MSTP mode.
- STP and Transparent Interconnection of Lots of Links (TRILL) of the data center cannot be enabled at the same time.

Configuration Steps

Enabling STP

- Mandatory.
- Unless otherwise specified, enable STP on each device.
- Run the **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*] command to enable STP and configure basic attributes.
- The forward-time ranges from 4 to 30. The hello-time ranges from 1 to 10. The max-age ranges from 6 to 40.

Running the **clear** commands may lose vital information and thus interrupt services. The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time –1 second). Otherwise, the configuration will fail.

Command	**spanning-tree** [**forward-time** *seconds*	**hello-time** *seconds*	**max-age** *seconds*	**tx-hold-count** *numbers*]
Parameter Description	**forward-time** *seconds*: Indicates the interval when the port status changes. The value ranges from 4 to 30 seconds. The default value is 15 seconds. **hello-time** *seconds*: Indicates the interval when a device sends a BPDU packet. The value ranges from 1 to 10 seconds. The default value is 2 seconds. **max-age** *second*: Indicates the longest TTL of a BPDU packet. The value ranges from 6 to 40 seconds. The default value is 20 seconds. **tx-hold-count** *numbers*: Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.
Defaults	STP is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time – 1 second) Otherwise, the topology may become unstable and the configuration will fail.

Configuring the STP Mode

- Optional.
- According to related 802.1 protocol standards, STP, RSTP, and MSTP are mutually compatible, without any configuration by the administrator. However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. Therefore, the device provides a command for the administrator to switch the STP mode to a lower version if other vendors' devices are incompatible with the device.
- Run the **spanning-tree mode** [**stp | rstp | mstp**] command to modify the STP mode.

Command	**spanning-tree mode** [**stp**	**rstp**	**mstp**]
Parameter De	**stp**: Spanning Tree Protocol (IEEE 802.1d)

scription	**rstp**: Rapid Spanning Tree Protocol (IEEE 802.1w) **mstp**: Multiple Spanning Tree Protocol (IEEE 802.1s)
Defaults	The default value is **mstp**.
Command Mode	Global configuration mode
Usage Guide	However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with devices, run this command to switch the STP mode to a lower version.

Verification

- Display the configuration.

Configuration Example

Enabling STP and Configuring Timer Parameters

Scenario **Figure 6-20**	
Configuration Steps	● Enable STP and set the STP mode to STP on the devices. ● Configure the timer parameters of root bridge DEV A as follows: Hello Time=4s, Max Age=25s, Forward Delay=18s.

DEV A	Step 1: Enable STP and set the STP mode to STP.
	`Hostname#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)#spanning-tree`
	`Hostname(config)#spanning-tree mode stp`
	Step 2: Configure the timer parameters of root bridge DEV A.
	`Hostname(config)#spanning-tree hello-time 4`
	`Hostname(config)#spanning-tree max-age 25`
	`Hostname(config)#spanning-tree forward-time 18`

DEV B	Enable STP and set the STP mode to STP.
	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#spanning-tree`
	`Hostname(config)#spanning-tree mode stp`

Verification	● Run the **show spanning-tree summary** command to display the spanning tree topology and protocol configuration parameters.

DEV A	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol stp`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec`
	
	`  Bridge ID  Priority    0`
	`             Address     00d0.f822.3344`
	`             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec`
	
	`Interface        Role Sts Cost       Prio     OperEdge Type`
	`---------------- ---- --- ---------- -------- -------- ----------------`
	`Gi0/2            Desg FWD 20000      128      False    P2p`
	`Gi0/1            Desg FWD 20000      128      False    P2p`

DEV B	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol stp`
	`  Root ID    Priority    0`
	`             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.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Altn BLK 20000      128      False    P2p Bound(STP)
Gi0/1            Root FWD 20000      128      False    P2p Bound(STP)
```

Common Errors

- The STP timer parameters will take effect only when the device is set as the root bridge of the STP.

6.4.2 Configuring STP Compatibility

Configuration Effect

- Enable the compatibility mode of a port to realize interconnection between our devices and other SPs' devices.
- Enable protocol migration to perform forcible version check to affect the compatibility between RSTP and STP.

Notes

- If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between our devices and other SPs' devices.

Configuration Steps

↘ Enabling the Compatibility Mode on a Port

- Optional.

Command	spanning-tree compatible enable
Parameter Description	N/A
Defaults	The compatibility mode is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between our devices and other SPs' devices.

↘ Enabling Protocol Migration

- Optional.
- If the peer device supports RSTP, you can enforce version check on the local device to force the two devices to run RSTP.
- Run the **clear spanning-tree detected-protocols** [**interface** *interface-id*] command to enforce version check on a port. For details, see "Compatibility Between RSTP and STP".

Command	**clear spanning-tree detected-protocols** [**interface** *interface-id*]
Parameter Description	**interface** *interface-id*: Indicates a port.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to enforce a port to send RSTP BPDU packets and perform forcible check on them.

Verification

- Display the configuration.

Configuration Example

Enabling STP Compatibility

Scenario Figure 6-21	
Configuration Steps	● Configure Instances 1 and 2 on Devices A and B, and map Instance 1 with VLAN 10 and Instance 2 with VLAN 20. ● Configure Gi0/1 and Gi0/2 to respectively belong to VLAN 10 and VLAN 20, and enable STP compatibility.

DEV A	Step 1: Configure Instances 1 and 2, and map Instances 1 and 2 respectively with VLANs 10 and 20.
	`Hostname#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)#spanning-tree mst configuration`
	`Hostname(config-mst)#instance 1 vlan 10`

	Hostname(config-mst)#instance 2 vlan 20 Step 2: Configure the VLAN the port belongs to, and enable STP compatibility on the port. Hostname(config)#int gi 0/1 Hostname(config-if-GigabitEthernet 0/1)#switchport access vlan 10 Hostname(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable Hostname(config-if-GigabitEthernet 0/1)#int gi 0/2 Hostname(config-if-GigabitEthernet 0/2)#switchport access vlan 20 Hostname(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable
DEV B	Perform the same steps as DEV A.
Verification	● Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated.
DEV A	Hostname#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 32768 Address 001a.a917.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 001a.a917.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p MST 1 vlans map : 10 Region Root Priority 32768

```
            Address     001a.a917.78cc
            this bridge is region root

  Bridge ID  Priority    32768
            Address     001a.a917.78cc

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Desg FWD 20000      128      False    P2p

MST 2 vlans map : 20
  Region Root Priority   32768
            Address     001a.a917.78cc
            this bridge is region root

  Bridge ID  Priority    32768
            Address     001a.a917.78cc

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Desg FWD 20000      128      False    P2p
```

DEV B

```
Hostname#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    32768
            Address     001a.a917.78cc
            this bridge is root
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
```

```
            Address     00d0.f822.3344
            Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Altn BLK 20000      128      False    P2p
Gi0/1            Root FWD 20000      128      False    P2p

MST 1 vlans map : 10
  Region Root Priority   32768
            Address     001a.a917.78cc
            this bridge is region root

  Bridge ID  Priority    32768
            Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Root FWD 20000      128      False    P2p

MST 2 vlans map : 20
  Region Root Priority   32768
            Address     001a.a917.78cc
            this bridge is region root

  Bridge ID  Priority    32768
            Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Root FWD 20000      128      False    P2p
```

Common Errors

N/A

6.4.3 Configuring an MSTP Region

Configuration Effect

- Configure an MSTP region to adjust which devices belong to the same MSTP region and thereby affect the network topology.

Notes

- To make multiple devices belong to the same MSTP region, configure the same name, revision number, and instance-VLAN mapping table for them.
- You can configure VLANs for Instances 0 to 64, and then the remaining VLANs are automatically allocated to Instance 0. One VLAN belongs to only one instance.
- It is recommended to configure the instance-VLAN mapping table after disabling STP. After the configuration, re-enable MSTP to ensure stability and convergence of the network topology.

Configuration Steps

↘ Configuring an MSTP Region

- Optional.
- Configure an MSTP region when multiple devices need to belong to the same MSTP region.
- Run the **spanning-tree mst configuration** command to enter the MST configuration mode.
- Run the **instance** *instance-id* **vlan** *vlan-range* command to configure the MSTI-VLAN mapping.
- Run the **name** *name* command to configure the MST name.
- Run the **revision** *version* command to configure the MST version number.

Command	**spanning-tree mst configuration**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to enter the MST configuration mode.

Command	**instance** *instance-id* **vlan** *vlan-range*
Parameter Description	*instance-id*: Indicates the MSTI ID, ranging from 0 to 64. *vlan-range*: Indicates the VLAN ID, ranging from 1 to 4,094.
Defaults	The default instance-VLAN mapping is that all VLANs are in Instance 0.

Command Mode	MST configuration mode
Usage Guide	To add a VLAN group to an MSTI, run this command. For example, instance 1 vlan 2-200: Adds VLANs 2 to 200 to Instance 1. instance 1 vlan 2,20,200: Adds VLANs 2, 20, and 200 to Instance 1. You can use the **no** form of this command to remove VLANs from an instance. Removed VLANs are automatically forwarded to Instance 0.

Command	**name** *name*
Parameter Description	*name*: Indicates the MST name. It consists of a maximum of 32 bytes.
Defaults	The default name is an empty character string.
Command Mode	MST configuration mode
Usage Guide	N/A

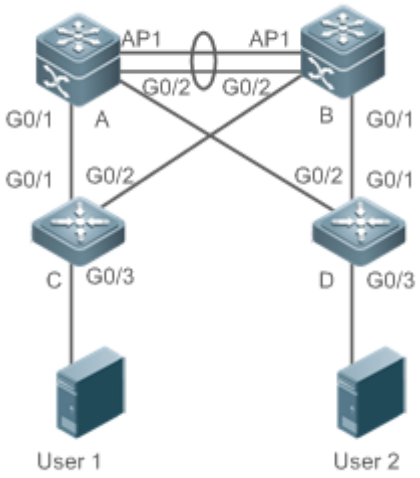
Command	**revision** *version*
Parameter Description	*version*: Indicates the MST revision number, ranging from 0 to 65,535.
Defaults	The default revision number is 0.
Command Mode	MST configuration mode
Usage Guide	N/A

Verification

- Display the configuration.
- Run the **show spanning-tree mst configuration** command to display the MSTP region configuration.

Configuration Example

↘ Enabling MSTP to Achieve VLAN Load Balancing in the MSTP+VRRP Topology

Scenario **Figure 6-22**	
Configuration Steps	● Enable MSTP and create Instances 1 and 2 on Switches A, B, C, and D. ● Configure Switch A as the root bridge of Instances 0 and 1 and Switch B as the root bridge of Instance 2. ● Configure Switch A as the VRRP master device of VLANs 1 and 10 and Switch B as the VRRP master device of VLAN 20.

A	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.
	`A(config)#vlan 10`
	`A(config-vlan)#vlan 20`
	`A(config-vlan)#exit`
	`A(config)#int range gi 0/1-2`
	`A(config-if-range)#switchport mode trunk`
	`A(config-if-range)#int ag 1`
	`A(config-if-AggregatePort 1)# switchport mode trunk`
	Step 2: Enable MSTP and create Instances 1 and 2.
	`A(config)#spanning-tree`
	`A(config)# spanning-tree mst configuration`
	`A(config-mst)#instance 1 vlan 10`
	`A(config-mst)#instance 2 vlan 20`
	`A(config-mst)#exit`
	Step 3: Configure Switch A as the root bridge of Instances 0 and 1.

```
A(config)#spanning-tree mst 0 priority 4096
A(config)#spanning-tree mst 1 priority 4096
A(config)#spanning-tree mst 2 priority 8192
```

Step 4: Configure VRRP priorities to enable Switch A to act as the VRRP master device of VLAN 10, and configure the virtual gateway IP address of VRRP.

```
A(config)#interface vlan 10
A(config-if-VLAN 10)ip address 192.168.10.2 255.255.255.0
A(config-if-VLAN 10) vrrp 1 priority 120
A(config-if-VLAN 10) vrrp 1 ip 192.168.10.1
```

Step 5 Set the VRRP priority to the default value 100 to enable Switch A to act as the VRRP backup device of VLAN 20.

```
A(config)#interface vlan 20
A(config-if-VLAN 20)ip address 192.168.20.2 255.255.255.0
A(config-if-VLAN 20) vrrp 1 ip 192.168.20.1
```

B

Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.

```
B(config)#vlan 10
B(config-vlan)#vlan 20
B(config-vlan)#exit
B(config)#int range gi 0/1-2
B(config-if-range)#switchport mode trunk
B(config-if-range)#int ag 1
B(config-if-AggregatePort 1)# switchport mode trunk
```

Step 2: Enable MSTP and create Instances 1 and 2.

```
B(config)#spanning-tree
B(config)# spanning-tree mst configuration
B(config-mst)#instance 1 vlan 10
B(config-mst)#instance 2 vlan 20
B(config-mst)#exit
```

	Step 3: Configure Switch A as the root bridge of Instance 2.
	`B(config)#spanning-tree mst 0 priority 8192`
	`B(config)#spanning-tree mst 1 priority 8192`
	`B(config)#spanning-tree mst 2 priority 4096`
	Step 4: Configure the virtual gateway IP address of VRRP.
	`B(config)#interface vlan 10`
	`B(config-if-VLAN 10)ip address 192.168.10.3 255.255.255.0`
	`B(config-if-VLAN 10) vrrp 1 ip 192.168.10.1`
	Step 5 Set the VRRP priority to 120 to enable Switch B to act as the VRRP backup device of VLAN 20.
	`B(config)#interface vlan 20`
	`B(config-if-VLAN 20)vrrp 1 priority 120`
	`B(config-if-VLAN 20)ip address 192.168.20.3 255.255.255.0`
	`B(config-if-VLAN 20) vrrp 1 ip 192.168.20.1`

C	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.
	`C(config)#vlan 10`
	`C(config-vlan)#vlan 20`
	`C(config-vlan)#exit`
	`C(config)#int range gi 0/1-2`
	`C(config-if-range)#switchport mode trunk`
	Step 2: Enable MSTP and create Instances 1 and 2.
	`C(config)#spanning-tree`
	`C(config)# spanning-tree mst configuration`
	`C(config-mst)#instance 1 vlan 10`
	`C(config-mst)#instance 2 vlan 20`
	`C(config-mst)#exit`
	Step 3: Configure the port connecting Device C directly to users as a PortFast port and enable BPDU guard.
	`C(config)#int gi 0/3`
	`C(config-if-GigabitEthernet 0/3)#spanning-tree portfast`

	C(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
D	Perform the same steps as Device C.
Verification	● Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated. ● Run the **show vrrp brief** command to check whether the VRRP master/backup devices are successfullycreated.
A	Hostname#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 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 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
  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
```

B

```
Hostname#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  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
  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
  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
```

C

```
Hostname#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  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
---------------- ---- --- ---------- -------- ----- --------------
Fa0/2            Altn BLK 200000     128      P2p   False
Fa0/1            Root FWD 200000     128      P2p   False

MST 1 vlans map : 10
  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
```

	---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Altn BLK 200000 128 P2p False Fa0/1 Root FWD 200000 128 P2p False MST 2 vlans map : 20 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 ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Root FWD 200000 128 P2p False Fa0/1 Altn BLK 200000 128 P2p False
D	Omitted.

Common Errors

- MST region configurations are inconsistent in the MSTP topology.
- VLANs are not created before you configure the mapping between the instance and VLAN.
- A device runs STP or RSTP in the MSTP+VRRP topology, but calculates the spanning tree according to the algorithms of different MST regions.

6.4.4 Enabling Fast RSTP Convergence

Configuration Effect

- Configure the link type to make RSTP rapidly converge.

Notes

- If the link type of a port is point-to-point connection, RSTP can rapidly converge. For details, see "Fast RSTP Convergence". If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port. If a port is in full duplex mode, the device sets the link type to point-to-point. If a port is in half duplex mode, the device sets the link type to shared. You can also forcibly configure the link type to determine whether the port connection is point-to-point connection.

Configuration Steps

Configuring the Link Type

- Optional.

Command	**spanning-tree link-type** [**point-to-point** | **shared**]
Parameter Description	**point-to-point**: Forcibly configures the link type of a port to be point-to-point. **shared**: Forcibly configures the link type of a port to be shared.
Defaults	If a port is in full duplex mode, the link type of the port is point-to-point. If a port is in half duplex mode, the link type of the port is shared.
Command Mode	Interface configuration mode
Usage Guide	If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Enabling Fast RSTP Convergence

Configuration Steps	Set the link type of a port to point-to-point.
	`Hostname(config)#int gi 0/1` `Hostname(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point`
Verification	● Run the **show spanning-tree summary** command to display the link type of the port.

	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : ALL`
	`  Root ID    Priority    32768`
	`            Address     001a.a917.78cc`
	`            this bridge is root`
	`            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`

```
  Bridge ID  Priority    32768
             Address     00d0.f822.3344
             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
```

Common Errors

N/A

6.4.5 Configuring Priorities

Configuration Effect

- Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.
- Configure the port priority to determine which port enters the forwarding state.

Notes

- It is recommended to set the priority of the core device higher (to a smaller value) to ensure stability of the entire network. You can assign different switch priorities to different instances so that each instance runs an independent STP based on the assigned priorities. Devices in different regions use the priority only of the CIST (Instance 0). As described in bridge ID, the switch priority has 16 optional values: 0, 4,096, 8,192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, 61,440. They are integral multiples of 4,096. The default value is 32,768.
- If two ports are connected to a shared device, the device selects a port with a higher priority (smaller value) to enter the forwarding state and a port with a lower priority (larger value) to enter the discarding state. If the two ports have the same priority, the device selects the port with a smaller port ID to enter the forwarding state. You can assign different port priorities to different instances on a port so that each instance runs an independent STP based on the assigned priorities.
- Similar to the switch priority, the port priority also has 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. They are integral multiples of 16. The default value is 128.

Configuration Steps

↘ Configuring the Switch Priority

- Optional.
- To change the root or topology of a network, configure the switch priority.

Command	**spanning-tree** [**mst** *instance-id*] **priority** *priority*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **priority** *priority*: Indicates the switch priority. There are 16 optional values: 0, 4,096, 8,192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, 61,440. They are integral multiples of 4,096.
Defaults	The default value of *instance-id* is 0 while that of *priority* is 32,768.
Command Mode	Global configuration mode
Usage Guide	Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

Configuring the Port Priority

- Optional.
- To change the preferred port entering the forwarding state, configure the port priority.

Command	spanning-tree [**mst** *instance-id*] **port-priority** *priority*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **port-priority** *priority*: Indicates the port priority. There are 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. They are integral multiples of 4,096.
Defaults	The default value of *instance-id* is 0. The default value of *priority* is 128.
Command Mode	Interface configuration mode
Usage Guide	If a loop occurs in a region, the port with a higher priority is preferred to enter the forwarding state. If two ports have the same priority, the port with a smaller port ID is selected to enter the forwarding state. Run this command to determine which port in the loop of a region enters the forwarding state.

Verification

- Displaythe configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Configuring the Port Priority

Scenario **Figure 6-23**	
Configuration Steps	● Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree. ● Configure the priority of Gi0/2 on DEV A is 16 so that Gi0/2 on DEV B can be selected as the root port.

DEV A	Step 1: Enable STP and configure the bridge priority.
	`Hostname(config)#spanning-tree`
	`Hostname(config)#spanning-tree mst 0 priority 0`
	Step 2: Configure the priority of Gi 0/2.
	`Hostname(config)# int gi 0/2`
	`Hostname(config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16`

DEV B	`Hostname(config)#spanning-tree`
Verification	● Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.

DEV A	`Hostname# Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : ALL`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`  Bridge ID  Priority    0`
	`             Address     00d0.f822.3344`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`

	Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 16 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	Hostname#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 001a.a917.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Root FWD 20000 128 False P2p Gi0/1 Altn BLK 20000 128 False P2p

Common Errors

N/A

6.4.6 Configuring the Port Path Cost

Configuration Effect

- Configure the path cost of a port to determine the forwarding state of the port and the topology of the entire network.
- If the path cost of a port uses its default value, configure the path cost calculation method to affect the calculation result.

Notes

- A device selects a port as the root port if the path cost from this port to the root bridge is the lowest. Therefore, the port path cost determines the root port of the local device. The default port path cost is automatically calculated based on the port rate (Media Speed). A port with a higher rate will have a low path cost. Since this method can calculate the most scientific path cost, do not change the path cost unless required. You can assign different path costs to different instances on a port so that each instance runs an independent STP based on the assigned path costs.
- If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate. However, IEEE 802.1d-1998 and IEEE 802.1t define different path costs for the same link rate. The value is a short integer ranging from 1 to 65,535 in 802.1d-1998 while is a long integer ranging from 1 to 200,000,000 in IEEE 802.1t. The path cost of an aggregate port (AP) has two solutions: 1. our solution: Port Path Cost x 95%; 2. Solution recommended in standards: 20,000,000,000/Actual link bandwidth of the AP, in which Actual link bandwidth of the AP = Bandwidth of a member port x Number of active member ports. The administrator must unify the path cost calculation method in the entire network. The default standard is the private long integer standard.
- The following table lists path costs automatically configured for different link rate in two solutions.

Port Rate	Port	IEEE 802.1d (short)	IEEE 802.1t (long)	IEEE 802.1t (long standard)
10M	Common port	100	2000000	2000000
	AP	95	1900000	2000000÷linkupcnt
100M	Common port	19	200000	200000
	AP	18	190000	200000÷linkupcnt
1000M	Common port	4	20000	20000
	AP	3	19000	20000÷linkupcnt
10000M	Common port	2	2000	2000
	AP	1	1900	20000÷linkupcnt

- Our long integer standard is used by default. After the solution is changed to the path cost solution recommended by the standards, the path cost of an AP changes with the number of member ports in UP state. If the port path cost changes, the network topology also will change.
- If an AP is static, linkupcnt in the table is the number of active member ports. If an AP is an LACP AP, linkupcnt in the table is the number of member ports forwarding AP data. If no member port in the AP goes up, linkupcnt is 1. For details about AP and LACP, see the *Configuring AP*.
- The modified port path cost takes effect only on the Rx port.

Configuration Steps

Configuring the Port Path Cost

- Optional.
- To determine which port or path data packets prefer to pass through, configure the port path cost.

Command	**spanning-tree** [**mst** *instance-id*] **cost** *cost*
Parameter De	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64.

scription	**cost** *cost*: Indicates the path cost, ranging from 1 to 200,000,000.
Defaults	The default value of *instance-id* is 0. The default value is automatically calculated based on the port rate. 1000 Mbps—20000 100 Mbps—200000 10 Mbps—2000000
Command Mode	Interface configuration mode
Usage Guide	A larger value of *cost* indicates a higher path cost.

Configuring the Default Path Cost Calculation Method

- Optional.
- To change the path cost calculation method, configure the default path cost calculation method.

Command	**spanning-tree pathcost method** { *long* [*standard*] | *short* }
Parameter Description	*long*: Uses the path cost specified in 802.1t. *standard*: Uses the cost calculated according to the standard. *short*: Uses the path cost specified in 802.1d.
Defaults	The path cost specified in 802.1t is used by default.
Command Mode	Global configuration mode
Usage Guide	If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Configuring the Port Path Cost

Scenario **Figure 6-24**	

Configuration Steps	● Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree. ● Configure the path cost of Gi 0/2 on DEV B is 1 so that Gi 0/2 can be selected as the root port.
DEV A	Hostname(config)#spanning-tree Hostname(config)#spanning-tree mst 0 priority 0
DEV B	Hostname(config)#spanning-tree Hostname(config)# int gi 0/2 Hostname(config-if-GigabitEthernet 0/2)# spanning-tree cost 1
Verification	● Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.

DEV A	Hostname# Hostname#show spanning-tree summary
	
	Spanning tree enabled protocol mstp
	MST 0 vlans map : ALL
	  Root ID Priority 0
	  Address 00d0.f822.3344
	  this bridge is root
	  Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec
	
	  Bridge ID Priority 0
	  Address 00d0.f822.3344
	  Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec
	
	Interface Role Sts Cost Prio OperEdge Type
	---------- ---- --- ---------- -------- -------- ----------
	Gi0/2 Desg FWD 20000 128 False P2p
	Gi0/1 Desg FWD 20000 128 False P2p

DEV B	Hostname#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL

```
  Root ID    Priority    0
             Address     00d0.f822.3344
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     001a.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Root FWD 1          128      False    P2p
Gi0/1            Altn BLK 20000      128      False    P2p
```

Common Errors

- N/A

6.4.7 Configuring the Maximum Hop Count of a BPDU Packet

Configuration Effect

- Configure the maximum hop count of a BPDU packet to change the BPDU TTL and thereby affect the network topology.

Notes

- The default maximum hop count of a BPDU packet is 20. Generally, it is not recommended to change the default value.

Configuration Steps

↘ Configuring the Maximum Hop Count

- (Optional) If the network topology is so large that a BPDU packet exceeds the default 20 hops, it is recommended to change the maximum hop count.

Command	**spanning-tree max-hops** *hop-count*
Parameter Description	*hop-count*: Indicates the number of devices a BPDU passes through before being discarded. It ranges from 1 to 40.
Defaults	The default value of *hop-count* is 20.
Command Mode	Global configuration mode
Usage Guide	In a region, the BPDU sent by the root bridge includes a hop count. Every time a BPDU passes through a

	device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU times out and the device discards the packet. This command specifies the number of devices a BPDU passes through in a region before being discarded. Changing the maximum hop count will affect all instances.

Verification

- Display the configuration.
- Run the **show spanning-tree max-hops** command to display the configured maximum hop count.

Configuration Example

Configuring the Maximum Hop Count of a BPDU Packet

Configuration Steps	• Set the maximum hop count of a BPDU packet to 25.
	`Hostname(config)# spanning-tree max-hops 25`
Verification	• Run the **show spanning-tree** command to display the configuration.

	`Hostname# show spanning-tree`
	`StpVersion : MSTP`
	`SysStpStatus : ENABLED`
	`MaxAge : 20`
	`HelloTime : 2`
	`ForwardDelay : 15`
	`BridgeMaxAge : 20`
	`BridgeHelloTime : 2`
	`BridgeForwardDelay : 15`
	`MaxHops: 25`
	`TxHoldCount : 3`
	`PathCostMethod : Long`
	`BPDUGuard : Disabled`
	`BPDUFilter : Disabled`
	`LoopGuardDef : Disabled`
	
	`###### mst 0 vlans map : ALL`
	`BridgeAddr : 00d0.f822.3344`

	Priority: 0 TimeSinceTopologyChange : 2d:0h:46m:4s TopologyChanges : 25 DesignatedRoot : 0.001a.a917.78cc RootCost : 0 RootPort : GigabitEthernet 0/1 CistRegionRoot : 0.001a.a917.78cc CistPathCost : 20000

6.4.8 Enabling PortFast-related Features

Configuration Effect

- After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.
- If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
- If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Notes

- The global BPDU guard takes effect only when PortFast is enabled on a port.
- If BPDU filter is enabled globally, a PortFast-enabled port neither sends nor receives BPDUs. In this case, the host connecting directly to the PortFast-enabled port does not receive any BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically fails.
- The global BPDU filter takes effect only when PortFast is enabled on a port.

Configuration Steps

↘ Enabling PortFast

- Optional.
- If a port connects directly to the network terminal, configure this port as a PortFast port.
- In global configuration mode, run the **spanning-tree portfast default** command to enable PortFast on all ports and the **no spanning-tree portfast default** command to disable PortFast on all ports.
- In interface configuration mode, run the **spanning-tree portfast** command to enable PortFast on a port and the **spanning-tree portfast disabled** command to disable PortFast on a port.

Command	**spanning-tree portfast default**
Parameter De	N/A

scription	
Defaults	PortFast is disabled on all ports by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**spanning-tree portfast**
Parameter De scription	N/A
Defaults	PortFast is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

Enabling BPDU Guard

- Optional.
- If device ports connect directly to network terminals, you can enable BPDU guard on these ports to prevent BPDU attacks from causing abnormality in the spanning tree topology. A port enabled with BPDU guard enters the error-disabled state after receiving a BPDU.
- If device ports connect directly to network terminals, you can enable BPDU guard to prevent loops on the ports. The prerequisite is that the downlink device (such as the hub) can forward BPDU packets.
- In global configuration mode, run the **spanning-tree portfast bpduguard default** command to enable BPDU guard on all ports and the **no spanning-tree portfast bpduguard default** command to disable BPDU guard on all ports.
- In interface configuration mode, run the **spanning-tree bpduguard enabled** command to enable BPDU guard on a port and the **spanning-tree bpduguard disabled** command to disable BPDU guard on a port.

Command	**spanning-tree portfast bpduguard default**
Parameter De scription	N/A
Defaults	BPDU guard is globally disabled by default.
Command Mode	Global configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU. Run the **show spanning-tree** command to display the configuration.

Command	**spanning-tree bpduguard enabled**
Parameter De	N/A

scription	
Defaults	BPDU guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.

Enabling BPDU Filter

- Optional.
- To prevent abnormal BPDU packets from affecting the spanning tree topology, you can enable BPDU filter on a port to filter abnormal BPDU packets.
- In global configuration mode, run the **spanning-tree portfast bpdufilter default** command to enable BPDU filter on all ports and the **no spanning-tree portfast bpdufilter default** command to disable BPDU filter on all ports.
- In interface configuration mode, run the **spanning-tree bpdufilter enabled** command to enable BPDU filter on a port and the **spanning-tree bpdufilter disabled** command to disable BPDU filter on a port.

Command	**spanning-tree portfast bpdufilter default**
Parameter Description	N/A
Defaults	BPDU filter is globally disabled by default.
Command Mode	Global configuration mode
Usage Guide	If BPDU filter is enabled, corresponding ports neither send nor receive BPDUs.

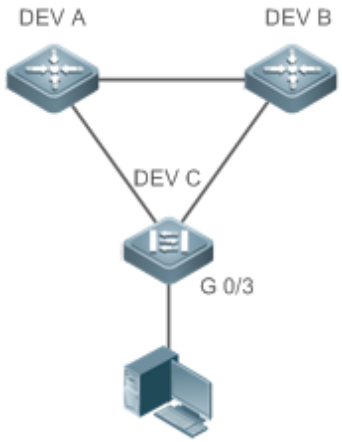
Command	**spanning-tree bpdufilter enabled**
Parameter Description	N/A
Defaults	BPDU filter is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Enabling PortFast on a Port

Scenario **Figure 6-25**	
Configuration Steps	● Configure Gi 0/3 of DEV C as a PortFast port and enable BPDU guard.
DEV C	Hostname(config)# int gi 0/3 Hostname(config-if-GigabitEthernet 0/3)# spanning-tree portfast %Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, switches, bridges to this interface when portfast is enabled,can cause temporary loops. Hostname(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
Verification	● Run the **show spanning-tree interface** command to displaythe port configuration.
DEV C	Hostname#show spanning-tree int gi 0/3 PortAdminPortFast : Enabled PortOperPortFast : Enabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Enabled PortAdminLinkType : auto PortOperLinkType : point-to-point PortBPDUGuard : Enabled PortBPDUFilter : Disabled PortGuardmode : None ###### MST 0 vlans mapped :ALL

	PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.00d0.f822.3344 PortDesignatedCost : 0 PortDesignatedBridge :0.00d0.f822.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 4 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

6.4.9 Enabling TC-related Features

Configuration Effect

- If TC protection is enabled on a port, the port deletes TC BPDU packets within a specified time (generally 4 seconds) after receiving them, preventing MAC and ARP entry from being removed.
- If TC guard is enabled, a port receiving TC packets filters TC packets received or generated by itself so that TC packets are not spread to other ports. In this way, possible TC attacks are efficiently prevented to keep the network stable.
- TC filter does not process TC packets received by ports but processes TC packets in case of normal topology changes.

Notes

- It is recommended to enable TC guard only when illegal TC attack packets are received in the network.

Configuration Steps

↘ Enabling TC Protection

- Optional.
- TC protection is disabled by default.
- In global configuration mode, run the **spanning-tree tc-protection** command to enable TC protection on all ports and the **no spanning-tree tc-protection** command to disable TC protection on all ports.
- TC protection can only be enabled or disabled globally.

Command	spanning-tree tc-protection
Parameter Description	N/A

Defaults	TC protection is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling TC Guard

- Optional.
- TC guard is disabled by default.
- To filter TC packets received or generated due to topology changes, you can enable TC guard.
- In global configuration mode, run the **spanning-tree tc-protection tc-guard** command to enable TC guard on all ports and the **no spanning-tree tc-protection tc-guard** command to disable TC guard on all ports.
- In interface configuration mode, run the **spanning-tree tc-guard** command to enable TC guard on a port and the **no spanning-tree tc-guard** command to disable TC guard on a port.

Command	**spanning-tree tc-protection tc-guard**
Parameter Description	N/A
Defaults	TC guard is globally disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enable TC guard to prevent TC packets from spreading.

Command	**spanning-tree tc-guard**
Parameter Description	N/A
Defaults	TC guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	Enable TC guard to prevent TC packets from spreading.

Enabling TC Filter

- Optional.
- TC filter is disabled by default.
- To filter TC packets received on a port, you can enable TC filter on the port.
- In interface configuration mode, run the **spanning-tree ignore tc** command to enable TC filter on a port and the **no spanning-tree ignore tc** command to disable it on a port.

Command	**spanning-tree ignore tc**
Parameter De	N/A

scription	
Defaults	TC filter is disabled bydefault.
Command Mode	Interface configuration mode
Usage Guide	If TC filter is enabled on a port, the port does not process received TC packets.

Verification

- Displaythe configuration.

Configuration Example

Enabling TC Guard on a Port

Configuration Steps	Enable TC guard on a port.
	`Hostname(config)#int gi 0/1` `Hostname(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard`
Verification	• Run the **show run interface** command to displaythe TC guard configuration of the port.

	`Hostname#show run int gi 0/1`
	
	`Building configuration...`
	`Current configuration : 134 bytes`
	
	`interface GigabitEthernet 0/1`
	` switchport mode trunk`
	` spanning-tree tc-guard`

Common Errors

- If TC guard or TC filter is incorrectly configured, an error may occur during packet forwarding of the network device. For example, when the topology changes, the device fails to clear MAC address in a timely manner, causing packet forwarding errors.

6.4.10 Enabling BPDU Source MAC Address Check

Configuration Effect

- Enable BPDU source MAC address check. After this, a device receives only BPDU packets with the source MAC address being the specified MAC address and discards other BPDU packets.

Notes

- When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check so that the switch receives the BPDU packets sent only by the peer switch.

Configuration Steps

Enabling BPDU Source MAC Address Check

- Optional.
- To prevent malicious BPDU attacks, you can enable BPDU source MAC address check.
- In interface configuration mode, run the **bpdu src-mac-check** *H.H.H* command to enable BPDU source MAC address check on a port and the **no bpdu src-mac-check** command to disable it on a port.

Command	**bpdu src-mac-check** *H.H.H*
Parameter Description	*H.H.H*: Indicates an MAC address. The device receives only BPDU packets with this address being the source MAC address.
Defaults	BPDU source MAC address check is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Verification

- Display the configuration.

Configuration Example

Enabling BPDU Source MAC Address Check on a Port

Configuration Steps	Enable BPDU source MAC address check on a port.
	`Hostname(config)#int gi 0/1` `Hostname(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 00d0.f800.1234`
Verification	● Run the **show run interface** command to display the spanning tree configuration of the port.

	`Hostname#show run int gi 0/1`
	
	`Building configuration...`
	`Current configuration : 170 bytes`

	interface GigabitEthernet 0/1 switchport mode trunk bpdu src-mac-check 00d0.f800.1234 spanning-tree link-type point-to-point

Common Errors

- If BPDU source MAC address check is enabled on a port, the port receives only BPDU packets with the configured MAC address being the source MAC address and discards all other BPDU packets.

6.4.11 Configuring Auto Edge

Configuration Effect

- Enable Auto Edge. If a designated port does not receive any BPDUs within a specified time (3 seconds), it is automatically identified as an edge port. However, if the port receives BPDUs, its Port Fast Operational State will become Disabled.

Notes

- Unless otherwise specified, do not disable Auto Edge.

Configuration Steps

↘ Configuring Auto Edge

- Optional.
- Auto Edge is enabled by default.
- In interface configuration mode, run the **spanning-tree autoedge** command to enable Auto Edge on a port and the **spanning-tree autoedge disabled** command to disable it on a port.

Command	**spanning-tree autoedge**
Parameter Description	N/A
Defaults	Auto Edge is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU. You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

Verification

- Displaythe configuration.

Configuration Example

Disabling Auto Edge on a Port

Configuration Steps	Disable Auto Edge on a port.
	Hostname(config)#int gi 0/1 Hostname(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled
Verification	● Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
	Hostname#show spanning-tree interface gi 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Disabled PortOperAutoEdge : Disabled PortAdminLinkType : point-to-point PortOperLinkType : point-to-point PortBPDUGuard : Disabled PortBPDUFilter : Disabled PortGuardmode : None ###### MST 0 vlans mapped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.00d0.f822.3344 PortDesignatedCost : 0 PortDesignatedBridge :0.00d0.f822.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 2 PortForwardTransitions : 6

	PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

Common Errors

If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. It is recommended to disable the Auto Edge function, if packet loss or Tx/Rx packet delay exists in the network environment.

6.4.12 Enabling Guard-related Features

Configuration Effect

- If root guard is enabled on a port, its roles on all instances are enforced as the designated port. Once the port receives configuration information with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive configuration information with a higher priority within a period, it returns to its original state.
- Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is to prevent this problem.

Notes

- Root guard and loop guard cannot take effect on a port at the same time.

Configuration Steps

↘ Enabling Root Guard

- Optional.
- The root bridge may receive configuration with a higher priority due to incorrect configuration by maintenance personnel or malicious attacks in the network. As a result, the current root bridge may lose its role, causing incorrect topology changes. To prevent this problem, you can enable root guard on a designated port of a device.
- In interface configuration mode, run the **spanning-tree guard root** command to enable root guard on a port and the **no spanning-tree guard root** command to disable it on a port.

Command	**spanning-tree guard root**
Parameter Description	N/A
Defaults	Root guard is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet

	attacks.

Enabling Loop Guard

- Optional.
- You can enable loop guard on a port (root port, master port, or AP) to prevent it from failing to receive BPDUs sent by the designated bridge, increasing device stability. Otherwise, the network topology will change, possibly causing a loop.
- In global configuration mode, run the **spanning-tree loopguard default** command to enable loop guard on all ports and the **no spanning-tree loopguard default** command to disable it on all ports.
- In interface configuration mode, run the **spanning-tree guard loop** command to enable loop guard on a port and the **no spanning-tree guard loop** command to disable it on a port.

Command	**spanning-tree loopguard default**
Parameter Description	N/A
Defaults	Loop guard is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Command	**spanning-tree guard loop**
Parameter Description	N/A
Defaults	Loop guard is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Disabling Guard

- Optional.

Command	**spanning-tree guard none**
Parameter Description	N/A
Defaults	Guard is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Displaythe configuration.

Configuration Example

↘ Enabling Loop Guard on a Port

Scenario **Figure 6-26**	
Configuration Steps	• Configure DEV A as the root bridge and DEV B as a non-root bridge on a spanning tree. • Enable loop guard on ports Gi 0/1 and Gi 0/2 of DEV B.
DEV A	Hostname(config)#spanning-tree Hostname(config)#spanning-tree mst 0 priority 0
DEV B	Hostname(config)#spanning-tree Hostname(config)# int range gi 0/1-2 Hostname(config-if-range)#spanning-tree guard loop
Verification	• Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
DEV A	Omitted.
DEV B	Hostname#show spanning-tree int gi 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 :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 0.001a.a917.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.001a.a917.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 17
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : rootPort

Hostname#show spanning-tree int gi 0/2

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 :ALL
PortState : discarding
PortPriority : 128
```

	PortDesignatedRoot : 0.001a.a917.78cc PortDesignatedCost : 0 PortDesignatedBridge :0.001a.a917.78cc PortDesignatedPortPriority : 128 PortDesignatedPort : 18 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : alternatePort

Common Errors

- If root guard is enabled on the root port, master port, or AP, the port may be incorrectly blocked.

6.4.13 Enabling BPDU Transparent Transmission

Configuration Effect

- If STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated.

Notes

- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Configuration Steps

↘ Enabling BPDU Transparent Transmission

- Optional.
- If STP is disabled on a device that needs to transparently transmit BPDU packets, enable BPDU transparent transmission.
- In global configuration mode, run the **bridge-frame forwarding protocol bpdu** command to enable BPDU transparent transmission and the **no bridge-frame forwarding protocol bpdu** command to disable it.
- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Command	**bridge-frame forwarding protocol bpdu**
Parameter Description	N/A

Defaults	BPDU transparent transmission is disabled by default.
Command Mode	Global configuration mode
Usage Guide	In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliant with IEEE 802.1Q do not forward the BPDU packets received. However, devices may need to transparently transmit BPDU packets in actual network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated. BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Verification

- Display the configuration.

Configuration Example

Enabling BPDU Transparent Transmission

Scenario Figure 6-27	
	STP is enabled on DEV A and DEV C while is disabled on DEV B.
Configuration Steps	● Enable BPDU transparent transmission on DEV B so that STP between DEV A and DEV C can be correctly calculated.
DEV B	`Hostname(config)#bridge-frame forwarding protocol bpdu`
Verification	● Run the **show run** command to check whether BPDU transparent transmission is enabled.

DEV B	`Hostname#show run`
	
	`Building configuration...`
	`Current configuration : 694 bytes`
	`bridge-frame forwarding protocol bpdu`

6.4.14 Enabling BPDU Tunnel

Configuration Effect

- Enable BPDU Tunnel so that STP packets from the customer network can be transparently transmitted across the SP network. STP packet transmission between the customer network does not affect the SP network, causing STP on the customer network to be calculated independently of that on the SP network.

Notes

- BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

Configuration Steps

↘ Enabling BPDU Tunnel

- (Optional) In a QinQ network, you can enable BPDU Tunnel if STP needs to be calculated separately between customer networks and SP networks.
- BPDU Tunnel is disabled by default.
- In global configuration mode, run the **l2protocol-tunnel stp** command to globally enable BPDU Tunnel and the **no l2protocol-tunnel stp** command to globally disable it.
- In interface configuration mode, run the **l2protocol-tunnel stp enable** command to enable BPDU Tunnel on a port and the **no l2protocol-tunnel stp enable** command to disable it on a port.
- Run the **l2protocol-tunnel stp tunnel-dmac** *mac-address* command in global configuration mode to configure the transparent transmission address of BPDU Tunnel.
- BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

Command	**l2protocol-tunnel stp**
Parameter Description	N/A
Defaults	BPDU Tunnel is disabled by default.
Command Mode	Global configuration mode
Usage Guide	BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

Command	**l2protocol-tunnel stp enable**
Parameter Description	N/A
Defaults	BPDU Tunnel is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	BPDU Tunnel takes effect only when it is enabled in both global configuration mode and interface configuration mode.

Command	**l2protocol-tunnel stp tunnel-dmac** *mac-address*
Parameter Description	*mac-address*: Indicates the STP address for transparent transmission.
Defaults	The default MAC address is 01d0.f800.0005.

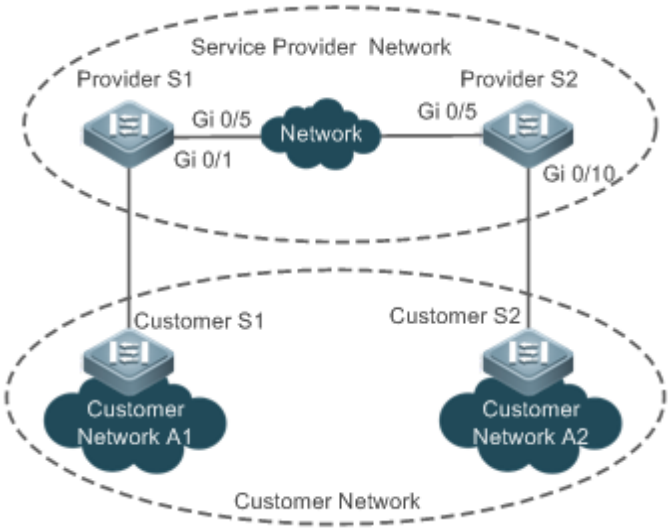
Command Mode	Global configuration mode
Usage Guide	If an STP packet sent from a customer network enters a PE, the PE changes the destination MAC address of the packet to a private address before the packet is forwarded by the SP network. When the packet reaches the PE at the peer end, the PE changes the destination MAC address to a public address and returns the packet to the customer network at the peer end, realizing transparent transmission across the SP network. This private address is the transparent transmission address of BPDU Tunnel. ⚠ Optional transparent transmission addresses of STP packets include 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2. ⚠ If no transparent transmission address is configured, BPDU Tunnel uses the default address 01d0.f800.0005.

Verification

- Run the **show l2protocol-tunnel stp** command to display the BPDU Tunnel configuration.

Configuration Example

Enabling BPDU Tunnel

Scenario Figure 6-28	
Configuration Steps	● Enable basic QinQ on the PEs (Provider S1/Provider S2 in this example) so that data packets of the customer network are transmitted within VLAN 200 on the SP network. ● Enable STP transparent transmission on the PEs (Provider S1/Provider S2 in this example) so that the SP network can transmit STP packets of the customer network through BPDU Tunnel.

Provider S1	Step 1: Create VLAN 200 on the SP network.
	`Hostname#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`

	Hostname(config)#vlan 200 Hostname(config-vlan)#exit Step 2: Enable basic QinQ on the port connected to the customer network and use VLAN 20 for tunneling. Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel Hostname(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 Hostname(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200 Step 3: Enable STP transparent transmission on the port connected to the customer network. Hostname(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable Hostname(config-if-GigabitEthernet 0/1)#exit Step 4: Enable STP transparent transmission in global configuration mode. Hostname(config)#l2protocol-tunnel stp Step 5: Configure an Uplink port. Hostname(config)# interface gigabitEthernet 0/5 Hostname(config-if-GigabitEthernet 0/5)#switchport mode uplink
Provider S2	Configure Provider S2 by performing the same steps.
Verification	● Check whether the BPDU Tunnel configuration is correct. ● Verify the Tunnel port configuration by checking whether: 1. The port type is dot1q-tunnel; 2. The outer tag VLAN is consistent with the native VLAN and added to the VLAN list of the Tunnel port; 3. The port that accesses the SP network is configured as an Uplink port.
Provider S1	Step 1: Check whether the BPDU Tunnel configuration is correct. Hostname#show l2protocol-tunnel stp L2protocol-tunnel: stp Enable L2protocol-tunnel destination mac address: 01d0.f800.0005 GigabitEthernet 0/1 l2protocol-tunnel stp enable Step 2: Check whether the QinQ configuration is correct. Hostname#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 200

	switchport dot1q-tunnel native vlan 200 l2protocol-tunnel stp enable spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink
Provider S2	Verify Provider S2 configuration by performing the same steps.

Common Errors

- In the SP network, BPDU packets can be correctly transparently transmitted only when the transparent transmission addresses of BPDU Tunnel are consistent.

6.5 Monitoring

Clearing

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

Description	Command
Clears the statistics of packets sent and received on a port.	**clear spanning-tree counters** [**interface** *interface-id*]
Clears the STP topology change information.	**clear spanning-tree mst** *instance-id* **topochange record**

Displaying

Description	Command
Displays MSTP parameters and spanning tree topology information.	**show spanning-tree**
Displays the count of sent and received MSTP packets.	**show spanning-tree counters** [**interface** *interface-id*]
Displays MSTP instances and corresponding port forwarding status.	**show spanning-tree summary**
Displays the ports that are blocked by root guard or loop guard.	**show spanning-tree inconsistentports**
Displays the configuration of an MST region.	**show spanning-tree mst configuration**
Displays MSTP information of an instance.	**show spanning-tree mst** *instance-id*
Displays MSTP information of the instance corresponding to a port.	**show spanning-tree mst** *instance-id* **interface** *interface-id*
Displays topology changes of a port in an instance.	**show spanning-tree mst** *instance-id* **topochange record**

Displays MSTP information of all instances corresponding to a port.	**show spanning-tree interface** *interface-id*
Displays the forwarding time.	**show spanning-tree forward-time**
Displays the hello time.	**show spanning-tree hello time**
Displays the maximum hop count.	**show spanning-tree max-hops**
Displays the maximum number of BPDU packets sent per second.	**show spanning-tree tx-hold-count**
Displays the path cost calculation method.	**show spanning-tree pathcost method**
Displays BPDU Tunnel information.	**show l2protocol-tunnel stp**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs all STPs.	**debug mstp all**
Debugs MSTP Graceful Restart (GR).	**debug mstp gr**
Debugs BPDU packet receiving.	**debug mstp rx**
Debugs BPDU packet sending.	**debug mstp tx**
Debugs MSTP events.	**debug mstp event**
Debugs loop guard.	**debug mstp loopguard**
Debugs root guard.	**debug mstp rootguard**
Debugs the bridge detection state machine.	**debug mstp bridgedetect**
Debugs the port information state machine.	**debug mstp portinfo**
Debugs the port protocol migration state machine.	**debug mstp protomigrat**
Debugs MSTP topology changes.	**debug mstp topochange**
Debugs the MSTP receiving state machine.	**debug mstp receive**
Debugs the port role transition state machine.	**debug mstp roletran**
Debugs the port state transition state machine.	**debug mstp statetran**
Debugs the MSTP sending state machine.	**debug mstp transmit**

7 Configuring LLDP

7.1 Overview

The Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is used to discover the 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, for example, which ports of a device are connected to other devices and whether the rates and duplex modes at both ends of a link are consistent. Administrators can quickly locate and rectify a fault based on the information.

An LLDP-compliant device is capable of discovering neighbors when the peer is either of the following:

- LLDP-compliant device
- Endpoint device that complies with the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)

Protocols and Standards

- IEEE 802.1AB 2005: Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

7.2 Applications

Application	Description
Displaying Topology	Multiple switches, a MED device, and an NMS are deployed in the network topology.
Conducting Error Detection	Two switches are directly connected and incorrect configuration will be displayed.

7.2.1 Displaying Topology

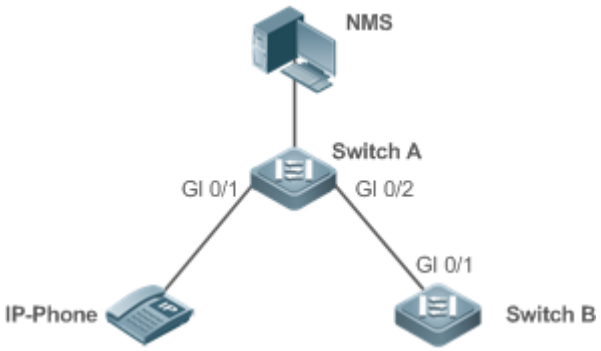
Scenario

Multiple switches, a MED device, and an NMS are deployed in the network topology.

As shown in the following figure, the LLDP function is enabled by default and no additional configuration is required.

- Switch A and Switch B discover that they are neighbors.
- Switch A discovers its neighbor MED device, that is, IP-Phone, through port GigabitEthernet 0/1.
- The NMS accesses MIB of switch A.

Figure 7-1



Remarks	Switch A, Switch B, and IP-Phone support LLDP and LLDP-MED. LLDP on switch ports works in TxRx mode. The LLDP transmission interval is 30 seconds and transmission delay is 2 seconds by default.

Deployment

- Run LLDP on a switch to implement neighbor discovery.
- Run the Simple Network Management Protocol (SNMP) on the switch so that the NMS acquires and sets LLDP-relevant information on the switch.

7.2.2 Conducting Error Detection

Scenario

Two switches are directly connected and incorrect configuration will be displayed.

As shown in the following figure, the LLDP function and LLDP error detection function are enabled by default, and no additional configuration is required.

- After you configure a virtual local area network (VLAN), port rate and duplex mode, link aggregation, and maximum transmission unit (MTU) of a port on Switch A, an error will be prompted if the configuration does not match that on Switch B, and vice versa.

Figure 7-2



Remarks	Switch A and Switch B support LLDP. LLDP on switch ports works in TxRx mode. The LLDP transmission interval is 30 seconds and transmission delay is 2 seconds by default.

Deployment

- Run LLDP on a switch to implement neighbor discovery and detect link fault.

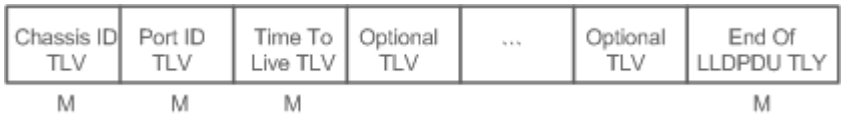
7.3 Features

Basic Concepts

LLDPDU

LLDPDU is a protocol data unit encapsulated into an LLDP packet. Each LLDPDU is a sequence of TLV structures. The TLV collection consists of three mandatory TLVs, a series of optional TLVs, and one End Of TLV. The following figure shows the format of an LLDPDU.

Figure 7-3 LLDPDU Format



In the preceding figure:

- M indicates a mandatory TLV.
- In an LLDPDU, Chassis ID TLV, Port ID TLV, Time To Live TLV, and End Of LLDPDU TLV are mandatory and TLVs of other TLVs are optional.

LLDP Encapsulation Format

LLDP packets can be encapsulated in two formats: Ethernet II and Subnetwork Access Protocols (SNAP).

The following figure shows the format of LLDP packets encapsulated in the Ethernet II format.

Figure 7-4 Ethernet II Format

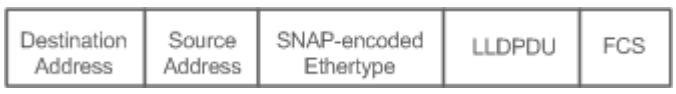


In the preceding figure:

- Destination Address: Indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.
- Source Address: Indicates the source MAC address, which is the port MAC address.
- Ethertype: Indicates the Ethernet type, which is 0x88CC.
- LLDPDU: Indicates the LLDP protocol data unit.
- FCS: Indicates the frame check sequence.

Figure 11-5 shows the format of LLDP packets encapsulated in the SNAP format.

Figure 7-5 SNAP Format



In the preceding figure:

- Destination Address: Indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.

- Source Address: Indicates the source MAC address, which is the port MAC address.
- SNAP-encoded Ethertype: Indicates the Ethernet type of the SNMP encapsulation, which is AA-AA-03-00-00-00-88-CC.
- LLDPDU: Indicates the LLDP protocol data unit.
- FCS: Indicates the frame check sequence.

TLV

TLVs encapsulated into an LLDPDU can be classified into two types:

- Basic management TLVs
- Organizationally specific TLVs

Basic management TLVs are a collection of basic TLVs used for network management. Organizationally specific TLVs are defined by standard organizations and other institutions, for example, the IEEE 802.1 organization and IEEE 802.3 organization define their own TLV collections.

1. Basic management TLVs

The basic management TLV 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.

The following table describes basic management TLVs.

TLV Type	Description	Mandatory/Optional
End Of LLDPDU TLV	Indicates the end of an LLDPDU, occupying two bytes.	Mandatory
Chassis ID TLV	Identifies a device with a MAC address.	Mandatory
Port ID TLV	Identifies a port sending LLDPDUs.	Fixed
Time To Live TLV	Indicates the time to live (TTL) of local information on a neighbor. When a device receives a TLV containing TTL 0, it deletes the neighbor information.	Mandatory
Port Description TLV	Indicates the descriptor of the port sending LLDPDUs.	Optional
System Name TLV	Describes the device name.	Optional
System Description TLV	Indicates the device description, including the hardware version, software version, and operating system information.	Optional
System Capabilities TLV	Describes main functions of the device, such as the bridge, routing, and relay functions.	Optional
Management Address TLV	Indicates the management address, which contains the interface ID and object identifier (OID).	Optional

LLDP-compliant switches support advertisement of basic management TLVs.

2. Organizationally specific TLVs

Different organizations, such as the IEEE 802.1, IEEE 802.3, IETF and device suppliers, define specific TLVs to advertise specific information about devices. The organizationally unique identifier (OUI) field in a TLV is used to distinguish different organizations.

- Organizationally specific TLVs are optional and are advertised in an LLDPDU selectively. Currently, there are three types of common organizationally specific TLVs: IEEE 802.1 organizationally specific TLVs, IEEE 802.3 organizationally specific TLVs, and LLDP-MED TLVs.

The following table describes IEEE 802.1 organizationally specific TLVs.

TLV Type	Description
Port VLAN ID TLV	Indicates the VLAN identifier of a port.
Port And Protocol VLAN ID TLV	Indicates the protocol VLAN identifier of a port.
VLAN Name TLV	Indicates the VLAN name of a port.
Protocol Identity TLV	Indicates the protocol type supported by a port.

LLDP-compliant switches do not send the Protocol Identity TLV but receive this TLV.

- IEEE 802.3 organizationally specific TLVs

The following table describes IEEE 802.3 organizationally specific TLVs.

TLV Type	Description
MAC/PHY Configuration//Status TLV	Indicates the rate and duplex mode of a port, and whether to support and enable auto-negotiation.
Power Via MDI TLV	Indicates the power supply capacity of a port.
Link Aggregation TLV	Indicates the link aggregation capacity of a port and the current aggregation state.
Maximum Frame Size TLV	Indicates the maximum size of the frame transmitted by a port.

LLDP-compliant devices support advertisement of IEEE 802.3 organizationally specific TLVs.

- LLDP-MED TLV

LLDP-MED is an extension to LLDP based on IEEE 802.1AB LLDP. It enables users to conveniently deploy the Voice Over IP (VoIP) network and detect faults. It provides applications including the network configuration policies, device discovery, PoE management, and inventory management, meeting requirements for low cost, effective management, and easy deployment.

The following table describes LLDP-MED TLVs.

TLV Type	Description
LLDP-MED Capabilities TLV	Indicates the type of the LLDP-MED TLV encapsulated into an LLDPDU and device type (network connectivity device or endpoint device), and whether to support LLDP-MED,.
Network Policy TLV	Advertises the port VLAN configuration, supported application type (such as voice or video services), and Layer-2 priority information.
Location Identification TLV	Locates and identifies an endpoint device.
Extended Power-via-MDI TLV	Provides more advanced power supply management.
Inventory – Hardware Revision TLV	Indicates hardware version of a MED device.
Inventory – Firmware Revision TLV	Indicates the firmware version of the MED device.

TLV Type	Description
Inventory – Software Revision TLV	Indicates the software version of the MED device.
Inventory – Serial Number TLV	Indicates the serial number of the MED device.
Inventory – Manufacturer Name TLV	Indicates the name of the manufacturer of the MED device.
Inventory – Model Name TLV	Indicates the module name of the MED device.
Inventory – Asset ID TLV	Indicates the asset identifier of the MED device, used for inventory management and asset tracking.

LLDP-compliant devices support advertisement of LLDP-MED TLVs.

Overview

Feature	Description
LLDP Work Mode	Configures the mode of transmitting and receiving LLDP packets.
LLDP Transmission Mechanism	Enables directly connected LLDP-compliant devices to send LLDP packets to the peer.
LLDP Reception Mechanism	Enables directly connected LLDP-compliant devices to receive LLDP packets from the peer.

7.3.1 LLDP Work Mode

Configure the LLDP work mode so as to specify the LLDP packet transmission and reception mode.

Working Principle

LLDP provides three work modes:

- TxRx: Transmits and receives LLDPDUs.
- Rx Only: Only receives LLDPDUs.
- Tx Only: Only transmits LLDPDUs.

When the LLDP work mode is changed, the port initializes the protocol state machine. You can set a port initialization delay to prevent repeated initialization of a port due to frequent changes of the LLDP work mode.

Related Configuration

Configuring the LLDP Work Mode

The default LLDP work mode is TxRx.

You can run the **lldp mode** command to configure the LLDP work mode.

If the work mode is set to TxRx, the device can both transmit and receive LLDP packets. If the work mode is set to Rx Only, the device can only receive LLDP packets. If the work mode is set to Tx Only, the device can only transmit LLDP packets. If the work mode is disabled, the device cannot transmit or receive LLDP packets.

7.3.2 LLDP Transmission Mechanism

LLDP packets inform peers of their neighbors. When the LLDP transmission mode is cancelled or disabled, LLDP packets cannot be transmitted to neighbors.

Working Principle

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 a delay time to avoid frequent transmission of LLDP packets caused by frequent changes of local information.
LLDP provides two types of packets:

- Standard LLDP packet, which contains management and configuration information about the local device.
- Shutdown packet: When the LLDP work mode is disabled or the port is shut down, LLDP Shutdown packets will be transmitted. A Shutdown packet consists of the Chassis ID TLV, Port ID TLV, Time To Live TLV, and End OF LLDP TLV. TTL in the Time to Live TLV is 0. When a device receives an LLDP Shutdown packet, it considers that the neighbor information is invalid and immediately deletes it.

When the LLDP work mode is changed from disabled or Rx to TxRx or Tx, or when 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 multiple LLDP packets at an interval of 1 second.

Related Configuration

↘ Configuring the LLDP Work Mode

The default work mode is TxRx.

Run the **lldp mode txrx** or **lldp mode tx** command to enable the LLDP packet transmission function. Run the **lldp mode rx** or **no lldp mode** command to disable the LLDP packet transmission function.

In order to enable LLDP packet reception, set the work mode to TxRx or Rx Only. If the work mode is set to Rx Only, the device can only receive LLDP packets.

↘ Configuring the LLDP Transmission Delay

The default LLDP transmission delay is 2 seconds.

Run the **lldp timer tx-delay** command to change the LLDP transmission delay.

If the delay is set to a very small value, the frequent change of local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed.

↘ Configuring the LLDP Transmission Interval

The default LLDP transmission interval is 30 seconds.

Run the **lldp timer tx-interval** command to change the LLDP transmission interval.

If the interval is set to a very small value, LLDP packets may be transmitted frequently. If the interval is set to a very large value, the peer may not discover the local device in time.

Configuring the TLVs to Be Advertised

By default, an interface is allowed to advertise TLVs of all types except Location Identification TLV.

Run the **lldp tlv-enable** command to change the TLVs to be advertised.

Configuring the LLDP Fast Transmission Count

By default, three LLDP packets are fast transmitted.

Run the **lldp fast-count** command to change the number of LLDP packets that are fast transmitted.

7.3.3 LLDP Reception Mechanism

A device can discover the neighbor and determine whether to age the neighbor information according to received LLDP packets.

Working Principle

A device can receive LLDP packets when working in TxRx or Rx Only mode. After receiving an LLDP packet, a device conducts validity check. After the packet passes the check, the device checks whether the packet contains information about a new neighbor or about 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 is aged immediately.

Related Configuration

Configuring the LLDP Work Mode

The default LLDP work mode is TxRx.

Run the **lldp mode txrx** or **lldp mode rx** command to enable the LLDP packet reception function. Run the **lldp mode tx** or **no lldp mode** command to disable the LLDP packet reception function.

In order to enable LLDP packet reception, set the work mode to TxRx or Rx Only. If the work mode is set to Tx Only, the device can only transmit LLDP packets.

7.4 Configuration

Configuration	Description and Command	
Configuring the LLDP Function	(Optional) It is used to enable or disable the LLDP function in global or interface configuration mode.	
	lldp enable	Enables the LLDP function.
	no lldp enable	Disables the LLDP function.

Configuration	Description and Command	
Configuring the LLDP Work Mode	(Optional) It is used to configure the LLDP work mode.	
	lldp mode {rx | tx | txrx}	Configures the LLDP work mode.
	no lldp mode	Shuts down the LLDP work mode.
Configuring the TLVs to Be Advertised	(Optional) It is used to configure the TLVs to be advertised.	
	lldp tlv-enable	Configures the TLVs to be advertised.
	no lldp tlv-enable	Cancels TLVs.
Configures the Management Address to Be Advertised	(Optional) It is used to configure the management address to be advertised in LLDP packets.	
	lldp management-address-tlv [*ip-address*]	Configures the management address to be advertised in LLDP packets.
	no lldp management-address-tlv	Cancels the management address.
Configuring the LLDP Fast Transmission Count	(Optional) It is used to configure the number of LLDP packets that are fast transmitted.	
	lldp fast-count *value*	Configures the LLDP fast transmission count.
	no lldp fast-count	Restores the default LLDP fast transmission count.
Configuring the TTL Multiplier and Transmission Interval	(Optional) It is used to configure the TTL multiplier and transmission interval.	
	lldp hold-multiplier *value*	Configures the TTL multiplier.
	no lldp hold-multiplier	Restores the default TTL multiplier.
	lldp timer tx-interval *seconds*	Configures the transmission interval.
	no lldp timer tx-interval	Restores the default transmission interval.
Configuring the Transmission Delay	(Optional) It is used to configure the delay time for LLDP packet transmission.	
	lldp timer tx-delay *seconds*	Configures the transmission delay.
	no lldp timer tx-delay	Restores the default transmission delay.
Configuring the Initialization Delay	(Optional) It is used to configure the delay time for LLDP to initialize on any interface.	
	lldp timer reinit-delay *seconds*	Configures the initialization delay.
	no lldp timer reinit-delay	Restores the default initialization delay.
Configuring the LLDP Trap Function	(Optional) It is used to configure the LLDP Trap function.	
	lldp notification remote-change enable	Enables the LLDP Trap function.
	no lldp notification remote-change enable	Disables the LLDP Trap function.
	lldp timer notification-interval	Configures the LLDP Trap transmission interval.

Configuration	Description and Command	
	no lldp timer notification-interval	Restores the default LLDP Trap transmission interval.
Configuring the LLDP Error Detection Function	(Optional) It is used to configure the LLDP error detection function.	
	lldp error-detect	Enables the LLDP error detection function.
	no lldp error-detect	Disables the LLDP error detection function.
Configuring the LLDP Encapsulation Format	(Optional) It is used to configure the LLDP encapsulation format.	
	lldp encapsulation snap	Sets the LLDP encapsulation format to SNAP.
	no lldp encapsulation snap	Sets the LLDP encapsulation format to Ethernet II.
Configuring the LLDP Network Policy	(Optional) It is used to configure the LLDP Network Policy.	
	lldp network-policy profile *profile-num*	Configures an LLDP Network Policy.
	no lldp network-policy profile *profile-num*	Deletes an LLDP Network Policy.
Configuring the Civic Address	(Optional) It is used to configure the civic address of a device.	
	{ **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*	Configures the civic address of a device.
	no { **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*	Deletes civic address of a device.
Configuring the Emergency Telephone Number	(Optional) It is used to configure the emergency telephone number of a device.	
	lldp location elin identifier *id* **elin-location** *tel-number*	Configures the emergency telephone number of a device.

Configuration	Description and Command	
	no lldp location elin identifier *id*	Deletes the emergency telephone number of a device.

7.4.1 Configuring the LLDP Function

Configuration Effect

- Enable or disable the LLDP function.

Notes

- To make the LLDP function take effect on an interface, you need to enable the LLDP function globally and on the interface.

Configuration Steps

- Optional.
- Configure the LLDP function in global or interface configuration mode.

Verification

Display LLDP status

- Check whether the LLDP function is enabled in global configuration mode.
- Check whether the LLDP function is enabled in interface configuration mode.

Related Commands

↘ Enabling the LLDP Function

Command	**lldp enable**
Parameter Description	N/A
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	The LLDP function takes effect on an interface only after it is enabled in global configuration mode and interface configuration mode.

↘ Disabling the LLDP Function

Command	**no lldp enable**
Parameter Description	N/A
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

Disabling the LLDP Function

Configuration Steps	Disable the LLDP function in global configuration mode.
	`Hostname(config)#no lldp enable`
Verification	Display global LLDP status.
	`Hostname(config)#show lldp status` `Global status of LLDP: Disable`

Common Errors

- If the LLDP function is enabled on an interface but disabled in global configuration mode, the LLDP function does not take effect on the interface.
- A port can learn a maximum of five neighbors.
- If a neighbor does not support LLDP but it is connected to an LLDP-supported device, a port may learn information about the device that is not directly connected to the port because the neighbor may forward LLDP packets.

7.4.2 Configuring the LLDP Work Mode

Configuration Effect

- If you set the LLDP work mode to TxRx, the interface can transmit and receive packets.
- If you set the LLDP work mode to Tx, the interface can only transmit packets but cannot receive packets.
- If you set the LLDP work mode to Rx, the interface can only receive packets but cannot transmit packets.
- If you disable the LLDP work mode, the interface can neither receive nor transmit packets.

Notes

- LLDP runs on physical ports (AP member ports for AP ports). Stacked ports and VSL ports do not support LLDP.

Configuration Steps

- Optional.
- Set the LLDP work mode to Tx or Rx as required.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Work Mode

Command	**lldp mode** { **rx** | **tx** | **txrx** }
Parameter Description	**rx**: Only receives LLDPDUs. **tx**: Only transmits LLDPDUs. **txrx**: Transmits and receives LLDPDUs.
Command Mode	Interface configuration mode
Usage Guide	To make LLDP take effect on an interface, make sure to enable LLDP globally and set the LLDP work mode on the interface to Tx, Rx or TxRx.

Disabling the LLDP Work Mode

Command	**no lldp mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	After the LLDP work mode on an interface is disabled, the interface does not transmit or receive LLDP packets.

Configuration Example

Configuring the LLDP Work Mode

Configuration Steps	Set the LLDP work mode to Tx in interface configuration mode.
	`Hostname(config)#interface gigabitethernet 0/1` `Hostname(config-if-GigabitEthernet 0/1)#lldp mode tx`
Verification	Display LLDP status information on the interface.

	`Hostname(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1`
	`Port [GigabitEthernet 0/1]`
	`Port status of LLDP : Enable`
	`Port state : UP`
	`Port encapsulation : Ethernet II`
	`Operational mode : TxOnly`
	`Notification enable : NO`

	Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

7.4.3 Configuring the TLVs to Be Advertised

Configuration Effect

- Configure the type of TLVs to be advertised to specify the LLDPDUs in LLDP packets.

Notes

- If you configure the **all** parameter for the basic management TLVs, IEEE 802.1 organizationally specific TLVs, and IEEE 802.3 organizationally specific TLVs, all optional TLVs of these types are advertised.
- If you configure the **all** parameter for the LLDP-MED TLVs, all LLDP-MED TLVs except Location Identification TLV are advertised.
- If you want to configure the LLDP-MED Capability TLV, configure the LLDP 802.3 MAC/PHY TLV first; If you want to cancel the LLDP 802.3 MAC/PHY TLV, cancel the LLDP-MED Capability TLV first.
- If you want to configure LLDP-MED TLVs, configure the LLDP-MED Capability TLV before configuring other types of LLDP-MED TLVs. If you want to cancel LLDP-MED TLVs, cancel the LLDP-MED Capability TLV before canceling other types of LLDP-MED TLVs If a device is connected to an IP-Phone that supports LLDP-MED, you can configure the Network Policy TLV to push policy configuration to the IP-Phone.
- If a device supports the DCBX function by default, ports of the device are not allowed to advertise IEEE 802.3 organizationally specific TLVs and LLDP-MED TLVs by default.

Configuration Steps

- Optional.
- Configure the type of TLVs to be advertised on an interface.

Verification

Display the configuration of TLVs to be advertised on an interface

- Check whether the configuration takes effect.

Related Commands

↘ Configuring TLVs to Be Advertised

Command	**lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } **|dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } **|dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location** { **civic-location** | **elin** } **identifier** *id* | **network-policy profile** [*profile-num*] |

	power-over-ethernet } }
Parameter Description	**basic-tlv**: Indicates the basic management TLV. **port-description**: Indicates the Port Description TLV. **system-capability**: Indicates the System Capabilities TLV. **system-description**: Indicates the System Description TLV. **system-name**: Indicates the System Name TLV. **dot1-tlv**: Indicates the IEEE 802.1 organizationally specific TLVs. **port-vlan-id**: Indicates the Port VLAN ID TLV. **protocol-vlan-id**: Indicates the Port And Protocol VLAN ID TLV. *vlan-id*: Indicates the Port Protocol VLAN ID, ranging from 1 to 4,094. **vlan-name**: Indicates the VLAN Name TLV. *vlan-id*: Indicates the VLAN name, ranging from 1 to 4,094. **dot3-tlv**: Indicates the IEEE 802.3 organizationally specific TLVs. **link-aggregation**: Indicates the Link Aggregation TLV. **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV. **max-frame-size**: Indicates the Maximum Frame Size TLV. **power**: Indicates the Power Via MDI TLV. **med-tlv**: Indicates the LLDP MED TLV. **capability**: Indicates the LLDP-MED Capabilities TLV. **Inventory**: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location**: Indicates the Location Identification TLV. **civic-location**: Indicates the civic address information and postal information. **elin**: Indicates the emergency telephone number. *id*: Indicates the policy ID, ranging from 1 to 1,024. **network-policy**: Indicates the Network Policy TLV. *profile-num*: Indicates the Network Policy ID, ranging from 1 to 1,024. **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Canceling TLVs

Command	**no lldp tlv-enable {basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id | vlan-name** } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv { all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }
Parameter Description	**basic-tlv**: Indicates the basic management TLV. **port-description**: Indicates the Port Description TLV. **system-capability**: Indicates the System Capabilities TLV.

	system-description: Indicates the System Description TLV. **system-name**: Indicates the System Name TLV. **dot1-tlv**: Indicates the IEEE 802.1 organizationally specific TLVs. **port-vlan-id**: Indicates the Port VLAN ID TLV. **protocol-vlan-id**: Indicates the Port And Protocol VLAN ID TLV. **vlan-name**: Indicates the VLAN Name TLV. **dot3-tlv**: Indicates the IEEE 802.3 organizationally specific TLVs. **link-aggregation**: Indicates the Link Aggregation TLV. **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV. **max-frame-size**: Indicates the Maximum Frame Size TLV. **power**: Indicates the Power Via MDI TLV. **med-tlv**: Indicates the LLDP MED TLV. **capability**: Indicates the LLDP-MED Capabilities TLV. **Inventory**: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location**: Indicates the Location Identification TLV. **civic-location**: Indicates the civic address information and postal information. **elin**: Indicates the emergency telephone number. *id*: Indicates the policy ID, ranging from 1 to 1,024. **network-policy**: Indicates the Network Policy TLV. *profile-num*: Indicates the Network Policy ID, ranging from 1 to 1,024. **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring TLVs to Be Advertised

Configuration Steps	Cancel the advertisement of the IEEE 802.1 organizationally specific Port And Protocol VLAN ID TLV.
	`Hostname(config)#interface gigabitethernet 0/1` `Hostname(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id`
Verification	Display LLDP TLV configuration in interface configuration mode.

	`Hostname(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1`
	`LLDP tlv-config of port [GigabitEthernet 0/1]`
	`NAME STATUS DEFAULT`
	`------------------------------ ------ -------`

```
Basic optional TLV:
Port Description TLV              YES    YES
System Name TLV                    YES    YES
System Description TLV            YES    YES
System Capabilities TLV           YES    YES
Management Address TLV            YES    YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV                   YES    YES
Port And Protocol VLAN ID TLV    NO     YES
VLAN Name TLV                       YES    YES

IEEE 802.3 extend TLV:
MAC-Physic TLV                      YES    YES
Power via MDI TLV                  YES    YES
Link Aggregation TLV               YES    YES
Maximum Frame Size TLV             YES    YES

LLDP-MED extend TLV:
Capabilities TLV                    YES    YES
Network Policy TLV                  YES    YES
Location Identification TLV       NO     NO
Extended Power via MDI TLV        YES    YES
Inventory TLV                         YES    YES
```

7.4.4 Configures the Management Address to Be Advertised

Configuration Effect

- Configure the management address to be advertised in LLDP packets in interface configuration mode.
- After the management address to be advertised is cancelled, the management address in LLDP packets is subject to the default settings.

Notes

- LLDP runs on physical ports (AP member ports for AP ports). Stacked ports and VSL ports do not support LLDP.

Configuration Steps

- Optional.
- Configure the management address to be advertised in LLDP packets in interface configuration mode.

Verification

Display LLDP information on a local interface

- Check whether the configuration takes effect.

Related Commands

Configuring the Management Address to Be Advertised

Command	**lldp management-address-tlv** [*ip-address*]
Parameter Description	*ip-address*: Indicates the management address to be advertised in an LLDP packet.
Command Mode	Interface configuration mode
Usage Guide	A management address is advertised through LLDP packets by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port. If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.

Canceling the Management Address

Command	**no lldp management-address-tlv**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	A management address is advertised through LLDP packets by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port. If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.

Configuration Example

Configuring the Management Address to Be Advertised

Configuration	Set the management address to 192.168.1.1 on an interface.

Steps	
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
Verification	Display configuration on the interface.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1 Lldp local-information of port [GigabitEthernet 0/1] Port ID type : Interface name Port id : GigabitEthernet 0/1 Port description : GigabitEthernet 0/1 Management address subtype : ipv4 Management address : 192.168.1.1 Interface numbering subtype : ifIndex Interface number : 1 Object identifier : 802.1 organizationally information Port VLAN ID : 1 Port and protocol VLAN ID(PPVID) : 1 PPVID Supported : YES PPVID Enabled : NO VLAN name of VLAN 1 : VLAN0001 Protocol Identity : 802.3 organizationally information Auto-negotiation supported : YES Auto-negotiation enabled : YES PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode Operational MAU type : speed(100)/duplex(Full)

```
PoE support                    : NO
Link aggregation supported     : YES
Link aggregation enabled       : NO
Aggregation port ID            : 0
Maximum frame Size             : 1500


LLDP-MED organizationally information
Power-via-MDI device type      : PD
Power-via-MDI power source     : Local
Power-via-MDI power priority   :
Power-via-MDI power value      :
Model name                     : Model name
```

7.4.5 Configuring the LLDP Fast Transmission Count

Configuration Effect

- Configure the number of LLDP packets that are fast transmitted.

Configuration Steps

- Optional.
- Configure the number of LLDP packets that are fast transmitted in global configuration mode.

Verification

Displaying the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Fast Transmission Count

Command	**lldp fast-count** *value*
Parameter Description	*value*: Indicates the number of LLDP packets that are fast transmitted. The value ranges from 1 to 10. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default LLDP Fast Transmission Count

Command	no lldp fast-count
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the LLDP Fast Transmission Count

Configuration Steps	Set the LLDP fast transmission count to 5 in global configuration mode.
	Hostname(config)#lldp fast-count 5
Verification	Display the global LLDP status information.
	Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 5

7.4.6 Configuring the TTL Multiplier and Transmission Interval

Configuration Effect

- Configure the TTL multiplier.
- Configure the LLDP packet transmission interval.

Configuration Steps

- Optional.
- Perform the configuration in global configuration mode.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Configuring the TTL Multiplier

Command	**lldp hold-multiplier** *value*
Parameter Description	*value*: Indicates the TLL multiplier. The value ranges from 2 to 10. The default value is 4.
Command Mode	Global configuration mode
Usage Guide	In an LLDP packet. the value of Time To Live TLV is calculated based on the following formula: Time to Live TLV= TTL multiplier x Packet transmission interval + 1. Therefore, you can modify the Time to Live TLV in LLDP packets by configuring the TTL multiplier.

Restoring the Default TTL Multiplier

Command	**no lldp hold-multiplier**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In an LLDP packet, the value of Time To Live TLV is calculated based on the following formula: Time to Live TLV = TTL multiplier x Packet transmission interval + 1. Therefore, you can modify the Time to Live TLV in LLDP packets by configuring the TTL multiplier.

Configuring the Transmission Interval

Command	**lldp timer tx-interval** *seconds*
Parameter Description	*seconds*: Indicates the LLDP packet transmission interval. The value ranges from 5 to 32,768.
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default Transmission Interval

Command	**no lldp timer tx-interval**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the TTL Multiplier and Transmission Interval

Configuration Steps	Set the TTL multiplier to 3 and the transmission interval to 20 seconds. The TTL of local device information on neighbors is 61 seconds.
	Hostname(config)#lldp hold-multiplier 3 Hostname(config)#lldp timer tx-interval 20
Verification	Displaythe global LLDP status information.
	Hostname(config)#lldp hold-multiplier 3 Hostname(config)#lldp timer tx-interval 20 Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 20s Hold multiplier : 3 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

7.4.7 Configuring the Transmission Delay

Configuration Effect

- Configure the delay time for LLDP packet transmission.

Configuration Steps

- Optional.
- Perform the configuration in global configuration mode.

Verification

Displaying the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the Transmission Delay

Command	**lldp timer tx-delay** *seconds*
Parameter Description	*seconds*: Indicates the transmission delay. The value ranges from 1 to 8,192.
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Restoring the Default Transmission Delay

Command	**no lldp timer tx-delay**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Configuration Example

Configuring the Transmission Delay

Configuration Steps	Set the transmission delay to 3 seconds.
	`Hostname(config)#lldp timer tx-delay 3`
Verification	Display the global LLDP status information.

	`Hostname(config)#show lldp status`
	`Global status of LLDP : Enable`
	`Neighbor information last changed time :`
	`Transmit interval : 30s`
	`Hold multiplier : 4`
	`Reinit delay : 2s`
	`Transmit delay : 3s`
	`Notification interval : 5s`
	`Fast start counts : 3`

7.4.8 Configuring the Initialization Delay

Configuration Effect

- Configure the delay time for LLDP to initialize on any interface.

Configuration Steps

- Optional.
- Configure the delay time for LLDP to initialize on any interface.

Verification

Display the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the Initialization Delay

Command	**lldp timer reinit-delay** *seconds*
Parameter Description	*seconds*: Indicates the initialization delay. The value ranges from 1 to 10 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure the initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Restoring the Default Initialization Delay

Command	**no lldp timer reinit-delay**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Configuration Example

Configuring the Initialization Delay

Configuration Steps	Set the initialization delay to 3 seconds.
	`Hostname(config)#lldp timer reinit-delay 3`

Verification	Displaythe global LLDP status information.
	Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 3s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

7.4.9 Configuring the LLDP Trap Function

Configuration Effect

- Configure the interval for transmitting LLDP Trap messages.

Configuration Steps

Enabling the LLDP Trap Function

- Optional.
- Perform the configuration in interface configuration mode.

Configuring the LLDP Trap Transmission Interval

- Optional.
- Perform the configuration in global configuration mode.

Verification

DisplayLLDP status information

- Check whether the LLDP Trap function is enabled.
- Check whether the interval configuration takes effect.

Related Commands

Enabling the LLDP Trap Function

Command	lldp notification remote-change enable
Parameter Description	N/A

Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance

Disabling the LLDP Trap Function

Command	**no lldp notification remote-change enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance.

Configuring the LLDP Trap Transmission Interval

Command	**lldp timer notification-interval** *seconds*
Parameter Description	*seconds*: Indicates the interval for transmitting LLDP Trap messages. The value ranges from 5 to 3,600 seconds. The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure the LLDP Trap transmission interval to prevent frequent transmission of LLDP Trap messages. LLDP changes detected within this interval will be transmitted to the NMS server.

Restoring the LLDP Trap Transmission Interval

Command	**no lldp timer notification-interval**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the LLDP Trap transmission interval to prevent frequent transmission of LLDP Trap messages. LLDP changes detected within this interval will be transmitted to the NMS server.

Configuration Example

Enabling the LLDP Trap Function and Configuring the LLDP Trap Transmission Interval

Configuration Steps	Enable the LLDP Trap function and set the LLDP Trap transmission interval to 10 seconds.
	`Hostname(config)#lldp timer notification-interval 10` `Hostname(config)#interface gigabitethernet 0/1`

	Hostname(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Verification	Display LLDP status information.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 10s Fast start counts : 3 -- Port [GigabitEthernet 0/1] -- Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : YES Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

7.4.10 Configuring the LLDP Error Detection Function

Configuration Effect

- Enable the LLDP error detection function. When LLDP detects an error, the error is logged.
- Configure the LLDP error detection function to detect VLAN configuration at both ends of a link, port status, aggregate port configuration, MTU configuration, and loops.

Notes

N/A

Configuration Steps

- Optional.
- Enable or disable the LLDP error detection function in interface configuration mode.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Enabling the LLDP Error Detection Function

Command	lldp error-detect
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Disabling the LLDP Error Detection Function

Command	no lldp error-detect
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Configuration Example

Enabling the LLDP Error Detection Function

Configuration Steps	Enable the LLDP error detection function on interface GigabitEthernet 0/1.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp error-detect
Verification	Display LLDP status information on the interface.

```
Hostname(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

7.4.11 Configuring the LLDP Encapsulation Format

Configuration Effect

- Configure the LLDP encapsulation format.

Configuration Steps

- Optional.
- Configure the LLDP encapsulation format on an interface.

Verification

Display LLDP status information of an interface

- Check whether the configuration takes effect.

Related Commands

Setting the LLDP Encapsulation Format to SNAP

Command	lldp encapsulation snap
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Restoring the Default LLDP Encapsulation Format (Ethernet II)

Command	No lldp encapsulation snap

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Configuration Example

Setting the LLDP Encapsulation Format to SNAP

Configuration Steps	Set the LLDP encapsulation format to SNAP.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
Verification	Display LLDP status information on the interface.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Snap Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

7.4.12 Configuring the LLDP Network Policy

Configuration Effect

- Configure the LLDP Network Policy.
- If a device is connected to an IP-Phone that supports LLDP-MED, you can configure the Network Policy TLV to push policy configuration to the IP-Phone, which enables the IP-Phone to change the tag and QoS of voice streams. In addition to the LLDP Network Policy, perform the following steps on the device: 1. Enable the Voice VLAN function and add the port connected to the IP-Phone to the Voice VLAN. 2. Configure the port connected to the IP-Phone as a QoS trusted port (the trusted DSCP mode is recommended). 3. If 802.1X authentication is also enabled on the port,

configure a secure channel for the packets from the Voice VLAN. If the IP-Phone does not support LLDP-MED, enable the voice VLAN function and add the MAC address of the IP-Phone to the Voice VLAN OUI list manually.

- For the configuration of the QoS trust mode, see *Configuring IP QoS*; for the configuration of the Voice VLAN, see *Configuring Voice VLAN*; for the configuration of the secure channel, see *Configuring ACL*.

Configuration Steps

- Optional.
- Configure the LLDP Network Policy.

Verification

Displaying the LLDP network policy configuration.

- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Network Policy

Command	**lldp network-policy profile** *profile-num*
Parameter Description	*profile-num*: Indicates the ID of an LLDP Network Policy. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the **{ voice | voice-signaling } vlan** command to configure a specific network policy.

Deleting the LLDP Network Policy

Command	**no lldp network-policy profile** *profile-num*
Parameter Description	*profile-num*: Indicates the LLDP Network Policy ID. The value ranges from 1 to 1,024.
Command Mode	Interface configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the **{ voice | voice-signaling } vlan** command to configure a specific network policy.

Configuration Example

Configuring the LLDP Network Policy

Configuration Steps	Set the Network Policy TLV to 1 for LLDP packets to be advertised by port GigabitEthernet 0/1 and set the VLAN ID of the Voice application to 3, COS to 4, and DSCP to 6.

	Hostname#config Hostname(config)#lldp network-policy profile 1 Hostname(config-lldp-network-policy)# voice vlan 3 cos 4 Hostname(config-lldp-network-policy)# voice vlan 3 dscp 6 Hostname(config-lldp-network-policy)#exit Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
Verification	Displaythe LLDP network policy configuration on the local device.
	network-policy information: ------------------------- network policy profile :1 voice vlan 3 cos 4 voice vlan 3 dscp 6

7.4.13 Configuring the Civic Address

Configuration Effect

- Configure the civic address of a device.

Configuration Steps

- Optional.
- Perform this configuration in LLDP Civic Address configuration mode.

Verification

Displaythe LLDP civic address of the local device

- Check whether the configuration takes effect.

Related Commands

↘ Configuring the Civic Address of a Device

Command	Configure the LLDP civic address. Use the **no** option to delete the address. { **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*

Parameter Description	**country**: Indicates the country code, with two characters. CH indicates China. **state**: Indicates the CA type is 1. **county**: Indicates that the CA type is 2. **city**: Indicates that the CA type is 3. **division**: Indicates that the CA type is 4. **neighborhood**: Indicates that the CA type is 5. **street-group**: Indicates that the CA type is 6. **leading-street-dir**: Indicates that the CA type is 16. **trailing-street-suffix**: Indicates that the CA type is 17. **street-suffix**: Indicates that the CA type is 18. **number**: Indicates that the CA type is 19. **street-number-suffix**: Indicates that the CA type is 20. **landmark**: Indicates that the CA type is 21. **additional-location-information**: Indicates that the CA type is 22. **name**: Indicates that the CA type is 23. **postal-code**: Indicates that the CA type is 24. **building**: Indicates that the CA type is 25. **unit**: Indicates that the CA type is 26. **floor**: Indicates that the CA type is 27. **room**: Indicates that the CA type is 28. **type-of-place**: Indicates that the CA type is 29. **postal-community-name**: Indicates that the CA type is 30. **post-office-box**: Indicates that the CA type is 31. **additional-code**: Indicates that the CA type is 32. *ca-word*: Indicates the address.
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Deleting the Civic Address of a Device

Command	**no** { **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** }
Parameter Description	N/A
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Configuring the Device Type

Command	**device-type** *device-type*
Parameter Description	*device-type*: Indicates the device type. The value ranges from 0 to 2. The default value is 1. 0 indicates that the device type is DHCP server. 1 indicates that the device type is switch. 2 indicates that the device type is LLDP MED .
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the device type.

Restoring the Device Type

Command	**no device-type**
Parameter Description	N/A
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, restore the default settings.

Configuration Example

Configuring the Civic Address of a Device

Configuration Steps	Set the address of port GigabitEthernet 0/1 as follows: set country to CH, city to Fuzhou, and postal code to 350000.

	`Hostname#config`
	`Hostname(config)#lldp location civic-location identifier 1`
	`Hostname(config-lldp-civic)# country CH`
	`Hostname(config-lldp-civic)# city Fuzhou`
	`Hostname(config-lldp-civic)# postal-code 350000`

Verification	Display the LLDP civic address of port GigabitEthernet 0/1 1.

	`civic location information:`
	`-------------------------`
	`Identifier :1`
	`country :CH`
	`device type :1`
	`city :Fuzhou`
	`postal-code :350000`

7.4.14 Configuring the Emergency Telephone Number

Configuration Effect

- Configure the emergencytelephone number of a device.

Configuration Steps

- Optional.
- Perform this configuration in global configuration mode.

Verification

Displaythe emergencytelephone number of the local device

- Check whether the configuration takes effect.

Related Commands

Configuring the Emergency Telephone Number of a Device

Command	**lldp location elin identifier** *id* **elin-location** *tel-number*
Parameter Description	*id*: Indicates the identifier of an emergencytelephone number. The value ranges from 1 to 1,024. *tel-number*: Indicates emergencytelephone number, containing 10-25 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the emergencytelephone number.

Deleting the Emergency Telephone Number of a Device

Command	**no lldp location elin identifier** *id*
Parameter Description	*id*: Indicates the identifier of an emergencytelephone number. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Emergency Telephone Number of a Device

Configuration Steps	Set the emergencytelephone number of port GigabitEthernet 0/1 to 085285555556.
	Hostname#config Hostname(config)#lldp location elin identifier 1 elin-location 085283671111
Verification	Displaythe emergencytelephone number of port GigabitEthernet 0/1.

	elin location information: ------------------------- Identifier :1 elin number :085283671111

7.4.15 Configuring the Detection of Compatible Neighbors

Configuration Effect

- Enables detection of compatible neighbors function.

Configuration Steps

- Optional.
- Perform this configuration in global configuration mode.

Verification

Display the LLDP information.

- Check whether the configuration takes effect.

Related Commands

Enabling detection of compatible neighbors

Command	lldp compliance vendor
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling detection of compatible neighbors

Command	no lldp compliance vendor
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Detection of Compatible Neighbors

Configuration Steps	Configuring the detection of compatible neighbor.
	`Hostname(config)# lldp compliance vendor`
Verification	Displaythe LLDP information.

	`Hostname(config)#show lldp status`
	`Global status of LLDP : Enable`
	`Global vendor compliance : YES`

7.5 Monitoring

Clearing

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

Description	Command
Clears LLDP statistics.	**clear lldp statistics** [**interface** *interface-name*]
Clears LLDP neighbor information.	**clear lldp table** [**interface** *interface-name*]

Displaying

Description	Command
Displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.	**show lldp local-information** [**global** | **interface** interface-name]
Displays the LLDP civic address or emergency telephone number of a local device.	**show lldp location** { **civic-location | elin-location** } { **identifier** *id* **| interface** *interface-name* **|static** }
Displays LLDP information on a neighbor.	**show lldp neighbors [interface** *interface-name*][**detail**]
Displays the LLDP network policy configuration of the local device.	**show lldp network-policy** { **profile** [*profile-num*] | **interface** *interface-name* }
Displays LLDP statistics.	**show lldp statistics** [**global | interface** *interface-name*]
Displays LLDP status information.	**show lldp status** [**interface** *interface-name*]
Displays the configuration of TLVs to be advertised by a port.	**show lldp tlv-config** [**interface** *interface-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs LLDP error processing.	**debug lldp error**
Debugs LLDP event processing.	**debug lldp event**
Debugs LLDP hot backup processing.	**debug lldp ha**
Debugs the LLDP packet reception.	**debug lldp packet**
Debugs the LLDP state machine.	**debug lldp stm**

8 Configuring QinQ

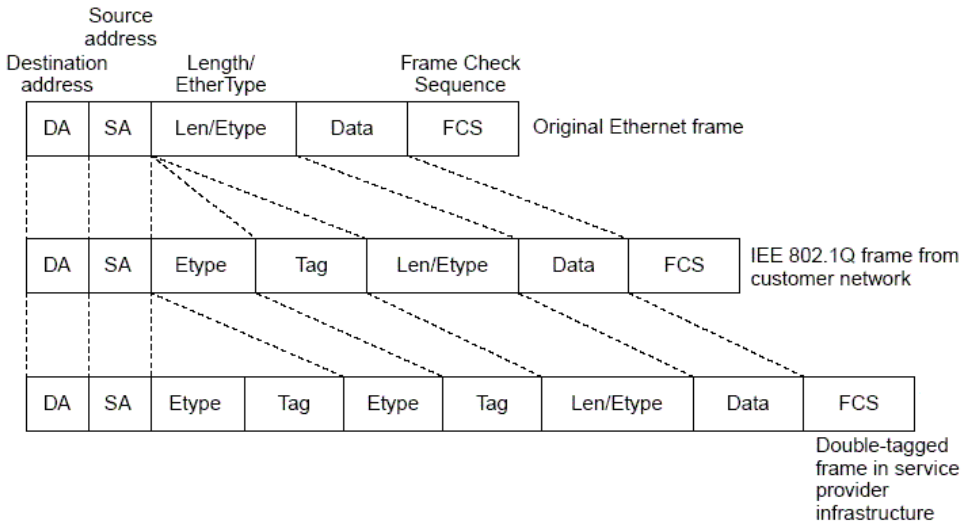
8.1 Overview

QinQ is used to insert a public virtual local area network (VLAN) tag into a packet with a private VLAN tag to allow the double-tagged packet to be transmitted over a service provider (SP) network.

Users on a metropolitan area network (MAN) must be separated by VLANs. IEEE 802.1Q supports only 4,094 VLANs, far from enough. Through the double-tag encapsulation provided by QinQ, a packet is transmitted over the SP network based on the unique outer VLAN tag assigned by the public network. In this way, private VLANs can be reused, which increases the number of available VLAN tags and provides a simple Layer-2 virtual private network (VPN) feature.

Figure 8-1 shows the double-tag insertion process. The entrance to an SP network is called a dot1q-tunnel port, or Tunnel port for short. All frames entering provider edges (PEs) are considered untagged. All tags, whether untagged frames or frames with customer VLAN tags, are encapsulated with the tags of the SP network. The VLAN ID of the SP network is the ID of the default VLAN for the Tunnel port.

Figure 8-1 Outer Tag Encapsulation



Protocols and Standards

- IEEE 802.1ad

8.2 Applications

Application	Description
Implementing Layer-2 VPN Through Port-Based Basic QinQ	Data is transmitted from Customer A and Customer B to the peer end without conflict on the SP network even if the data comes from the same VLAN.

Application	Description
Implementing Layer-2 VPN and Service Flow Management Through C-TAG-Based Selective QinQ	Outer tags are inserted into frames flexibly based on different customer VLANs to achieve Layer-2 VPN, segregate service flows (e.g., broadband Internet access and IPTV), and implement various QoS policies. Customer tag (C-TAG)-based QinQ is more flexible than port-based QinQ.
Implementing Layer-2 VPN and Service Flow Management Through ACL-Based Selective QinQ	The different service flows, such as broadband Internet access and IPTV, are segregated based on access control lists (ACLs). Different QoS policies are applied to service flows through selective QinQ.
Implementing QinQ-Based Layer-2 Transparent Transmission	Customer Network A and Customer Network B in different areas can perform unified Multiple Spanning Tree Protocol (MSTP) calculation or VLAN deployment across the SP network without affecting the SP network.

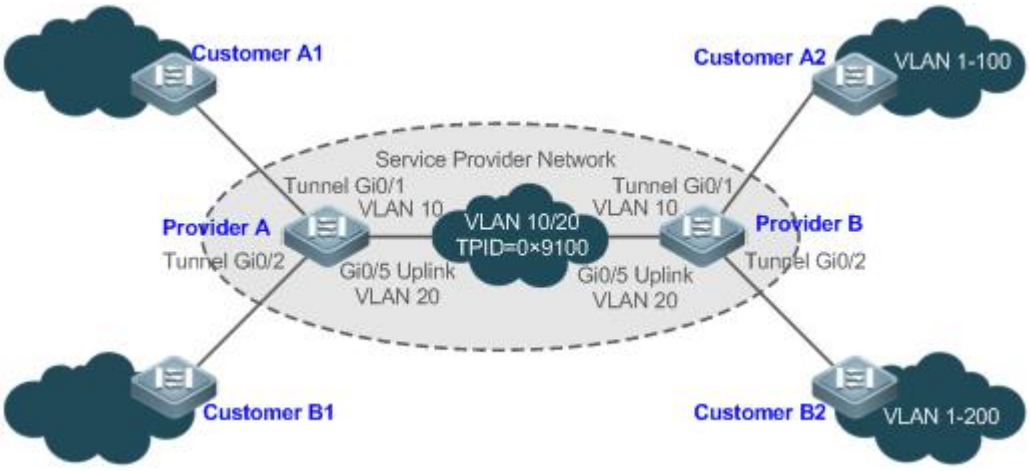
8.2.1 Implementing Layer-2 VPN Through Port-Based Basic QinQ

Scenario

An SP provides the VPN service to Customer A and Customer B.

- Customer A and Customer B belong to different VLANs on the SP network and achieve communication through respective SP VLANs.
- The VLANs of Customer A and Customer B are transparent to the SP network. The VLANs can be reused without conflicts.
- The Tunnel port encapsulates a native VLAN tag in each packet. Packets are transmitted through the native VLAN over the SP network without impact on the VLANs of Customer A and Customer B, thus implementing simple Layer-2 VPN.

Figure 8-2



Remarks	Customer A1 and Customer A2 are the customer edges (CEs) for Customer A network. Customer B1 and Customer B2 are the CEs for Customer B network. Provider A and Provider B are the PEs on the SP network. Customer A and Customer B access the SP network through Provider A and Provider B. The VLAN of Customer A ranges from 1 to100.

	The VLAN of Customer B ranges from 1 to 200.

Deployment

- Enable basic QinQ on PEs to implement Layer-2 VPN.
- The tag protocol identifiers (TPIDs) used by many switches (including our switches) are set to 0x8100, but the switches of some vendors do not use 0x8100. In the latter case, you need to change the TPID value on the Uplink ports of PEs to the values of the TPIDs used by third-party switches.
- Configure priority replication and priority mapping for class of service (CoS) on the Tunnel ports of PEs, and configure different QoS policies for different service flows (for details, see *Configuring QoS*).

8.2.2 Implementing Layer-2 VPN and Service Flow Management Through C-TAG-Based Selective QinQ

Scenario

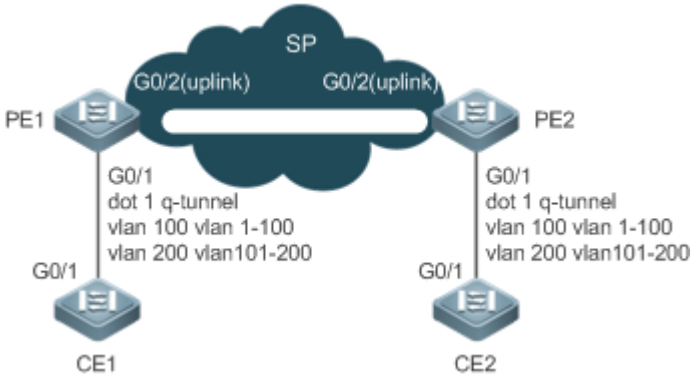
Basic QinQ encapsulates an outer tag of the native VLAN in a packet. That is, the encapsulation of outer tags depends on the native VLAN on Tunnel ports. Selective QinQ encapsulates an outer tag in a packet based on its inner tag to implement VPN transparent transmission and apply QoS policies flexibly.

- Broadband Internet access and IPTV are important services carried by MANs. The SPs manage different service flows through different VLANs and provides QoS policies for the VLANs or CoS. You can enable C-TAG-based QinQ on PEs to encapsulate outer VLAN tags in the service flows to achieve transparent transmission based on the QoS policies of the SP network.
- Important services and regular services are separated within different VLAN ranges. The customer can transmit service flows transparently over an SP network through C-TAG-based selective QinQ and ensure preferential transmission of important service flows by using the QoS policies of the SP network.

In Figure 8-3, the CEs are aggregated by the floor switches inside residential buildings. The broadband Internet access and IPTV services are segregated by VLANs with different QoS policies.

- The service flows of broadband Internet access and IPTV are transmitted transparently by different VLANs over the SP network.
- The SP network provides QoS policies based on VLANs or CoS. On the PEs, you can encapsulate an outer tag in the service flow based on its inner VLAN tag or set a CoS to ensure preferential transmission of service flows over the SP network.
- The CoS values of service packets can be changed through priority mapping or replication so that the QoS policies of the SP network are applied flexibly.

Figure 8-3



Remarks	CE 1 and CE 2 access the SP network through PE1 and PE2. On CE 1 and CE 2, the broadband Internet access flows are transmitted through VLAN 1–100, and IPTV flows are transmitted through VLAN 101–200. PE 1 and PE 2 are configured with Tunnel ports and VLAN mappings to segregate service flows.

Deployment

- Configure C-TAG-based selective QinQ on the ports (G0/1) of PE 1 and PE 2 connected to CE 1 and CE 2 respectively to realize the segregation and transparent transmission of service flows.
- If the SP network provides QoS policies based on VLANs or CoS, you can encapsulate an outer tag in the service flow based on its inner tag or set a CoS through priority replication or mapping on PE 1 and PE 2 to ensure preferential transmission of service flows over the SP network.

8.2.3 Implementing Layer-2 VPN and Service Flow Management Through ACL-Based Selective QinQ

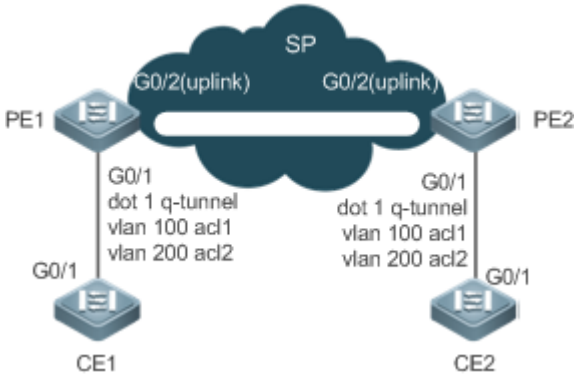
Scenario

The service flows from the customer network may be classified by MAC address, IP address, or protocol type, instead of by VLAN. The customer network may contain many low-end access devices unable to segregate service flows by VLAN IDs. In the preceding two situations, the packets from the customer network cannot be encapsulated with outer tags based on their inner tags to realize transparent transmission and implement QoS policies. Service flows may be classified by MAC address, IP address, or protocol type through ACLs. Selective QinQ uses ACLs to segregate service flows and add or modify outer tags in order to implement Layer-2 VPN and QoS policies based on different service flows.

In Figure 8-4, different VLANs are configured on PE 1 and PE 2 to transmit different service flows classified through ACLs. If the SP network provides QoS policies based on different services, certain services can be transmitted preferentially.

- Outer VLAN tags are encapsulated based on different service flows. The service flows of a customer network can be transmitted transparently, and its branch offices can access each other.
- The SP network provides QoS policies based on the VLAN tags or CoS values to ensure preferential transmission of certain service flows.

Figure 8-4



Remarks	CE 1 and CE 2 access the SP network through PE1 and PE2. PE 1 and PE 2 classify flows based on ACLs: ACL 1 matches the Point-to-Point Protocol over Ethernet (PPPoE) flows, and ACL 2 matches the IPTV flows. PE 1 and PE 2 are configured with Tunnel ports, as well as outer tag encapsulation policies applicable to service flows recognized by different ACLs.

Deployment

- Configure ACLs on PE 1 and PE 2 to segregate service flows.
- Configure ACL-based selective QinQ on the ports (G0/1) of PE 1 and PE 2 connected to CE 1 and CE 2 respectively to realize the segregation and transparent transmission of service flows.
- If the SP network provides QoS policies based on VLANs or CoS, you can encapsulate an outer tag in the service flow based on its inner tag or set a CoS through priority replication or mapping on PE 1 and PE 2 to ensure preferential transmission of service flows over the SP network.

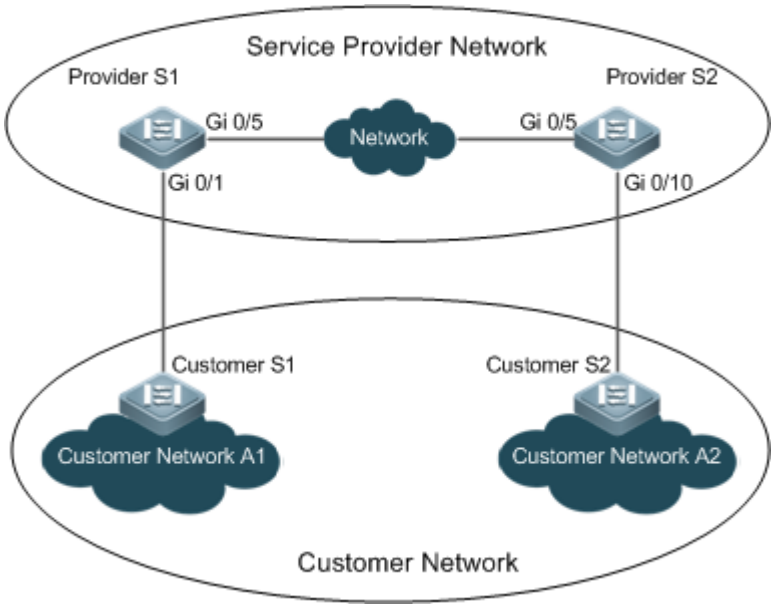
8.2.4 Implementing QinQ-Based Layer-2 Transparent Transmission

Scenario

The Layer-2 transparent transmission between customer networks has no impact on the SP network.

- The Layer-2 packets on customer networks are transparent to SP networks and can be transmitted between the customer networks without impact on the SP networks.

Figure 8-5



Remarks	Customer S1 and Customer S2 access the SP network through Provider S1 and Provider S2. Provider S1 and Provider S2 are enabled with Layer-2 transparent transmission globally, and the Gi 0/1 and Gi 0/10 ports are enabled with Layer-2 transparent transmission.

Deployment

- On the ports of the PEs (Provider S1 and Provider S2) connected to Customer S1 and Customer S2 respectively, configure Layer-2 transparent transmission between Customer Network A1 and Customer Network A2 without impact on the SP network.
- Configure STP transparent transmission based on user requirements to realize transparent transmission of bridge protocol data unit (BPDU) packets between Customer Network A1 and Customer Network A2 and to perform unified MSTP calculation across the SP network.
- Configure GARP VLAN Registration Protocol (GVRP) transparent transmission based on user requirements to realize transparent transmission of GVRP packets between Customer Network A1 and Customer Network A2 and dynamic VLAN configuration on the customer networks across the SP network.

8.3 Features

Basic Concepts

Basic QinQ

Configure basic QinQ on a Tunnel port and configure a native VLAN for the port. Packets entering the port are encapsulated with outer tags containing the native VLAN ID. Basic QinQ does not segregate service flows and cannot encapsulate packets flexibly based on VLANs.

Selective QinQ

Selective QinQ is classified into two types: selective QinQ based on C-TAGs and selective QinQ based on ACLs.
In C-TAG-based selective QinQ, outer tags are encapsulated in packets based on the inner tags to segregate service flows and realize transparent transmission.
In ACL-based selective QinQ, outer tags are encapsulated in packets based on the ACLs to segregate service flows.

TPID

An Ethernet frame tag consists of four fields: TPID, User Priority, Canonical Format Indicator (CFI), and VLAN ID.
By default, the TPID is 0x8100 according to IEEE802.1Q. On the switches of some vendors, the TPID is set to 0x9100 or other values. The TPID configuration aims to ensure that the TPIDs of packets to be forwarded are compatible with the TPIDs supported by third-party switches.

Priority Mapping and Priority Replication

The default value of User Priority in Ethernet frame tags is 0, indicating regular flows. You can set this field to ensure preferential transmission of certain packets. You can specify User Priority by setting the value of CoS in a QoS policy.
Priority replication: If the SP network provides a QoS policy corresponding to a specified CoS in the inner tag, you can replicate the CoS of the inner tag to the outer tag to enable transparent transmission based on the QoS policy provided by the SP network.
Priority mapping: If the SP network provides various QoS policies corresponding to specified CoS values for different service flows, you can map the CoS value of the inner tag to the CoS value of the outer tag to ensure preferential transmission of service flows based on the QoS policies provided by the SP network.

Layer-2 Transparent Transmission

STP and GVRP packets may affect the topology of the SP network. If you want to unify the topology of two customer networks separated by the SP network without affecting the SP network topology, transmit the STP and GVRP packets from the customer networks over the SP network transparently.

Overview

Feature	Description
Basic QinQ	Configures the Tunnel port and specifies whether packets sent from the port are tagged.
Selective QinQ	Encapsulates different outer tags in data flows based on ACLs.
TPID Configuration	By default, the TPID is 0x8100 according to IEEE802.1Q. On the switches of some vendors, the TPIDs of outer tags are set to 0x9100 or other values. The TPID configuration aims to ensure that the TPIDs of packets to be forwarded are compatible with the TPIDs supported by third-party switches.
MAC Address Replication	In ACL-based selective QinQ, the VLAN IDs for the MAC addresses that switches learn belong to the native VLAN. If VLAN conversion is implemented based on ACLs, upon receiving packets from the peer end, the local end may fail to query MAC addresses, causing a flood. To address this problem, MAC address replication is provided to replicate the MAC addresses of the native VLAN to the VLAN where the outer tag is located.
Layer-2 Transparent Transmission	Transmits Layer-2 packets between customer networks without impact on SP networks.

Feature	Description
Priority Replication	If the SP network provides a QoS policy corresponding to a specified CoS value in the inner tag, you can replicate the CoS of the inner tag to the outer tag to enable transparent transmission based on the QoS policy provided by the SP network.
Priority Mapping	If the SP network provides various QoS policies corresponding to specified CoS values for different service flows, you can map the CoS value of the inner tag to the CoS value of the outer tag to ensure preferential transmission of service flows based on the QoS policies provided by the SP network.

8.3.1 Basic QinQ

Basic QinQ can be used to implement simple Layer-2 VPN, but it lacks flexibility in encapsulating outer tags.

Working Principle

After a Tunnel port receives a packet, the switch adds the outer tag containing the default VLAN ID to the packet. If the received packet already carries a VLAN tag, it is encapsulated as a double-tagged packet. If it does not have a VLAN tag, it is added with the VLAN tag containing the default VLAN ID.

8.3.2 Selective QinQ

Selective QinQ adds different outer tags to data flows flexibly.

Working Principle

Selective QinQ can be used to encapsulate different outer tags based on inner tags, MAC addresses, protocol numbers, source addresses, destination addresses, priorities, or the port numbers of applications. In this way, packets of different users, services, and priorities are encapsulated with different outer VLAN tags.

You can configure the following selective QinQ policies:

- Add an outer VLAN tag based on the inner VLAN tag.
- Modify an outer VLAN tag based on the outer VLAN tag.
- Modify an outer VLAN tag based on the inner VLAN tag.
- Modify an outer VLAN tag based on the inner and outer VLAN tags.
- Add an outer VLAN tag based on the ACL.
- Modify an outer VLAN tag based on the ACL.
- Modify an inner VLAN tag based on the ACL.

8.3.3 TPID Configuration

Working Principle

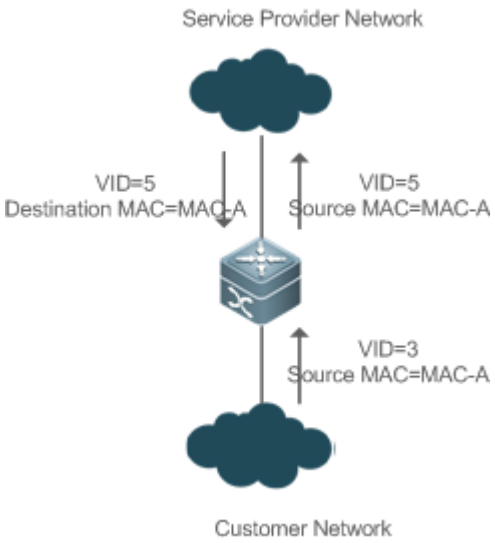
An Ethernet frame tag consists of four fields, namely, TPID, User Priority, CFI, and VLAN ID. By default, the TPID is 0x8100 according to IEEE802.1Q. On the switches of some vendors, the TPIDs of outer tags are set to 0x9100 or other values. The TPID configuration feature allows you to configure TPIDs on ports, which will replace the TPIDs of the outer VLAN tags in packets with the configured TPIDs to realize TPID compatibility.

8.3.4 MAC Address Replication

Working Principle

In ACL-based selective QinQ, the MAC address learned by a switch belongs to the native VLAN. The Tunnel port tags the packet with the specified outer VLAN ID based on the selective QinQ policy. Upon receiving a reply packet containing the same outer VLAN tag, the Tunnel port fails to find the MAC address in the outer VLAN as it is in the native VLAN, causing a flood.

Figure 8-6



As in Figure 8-6, the customer network is connected to the Tunnel port of the switch. Configured with native VLAN 4, the Tunnel port tags the packet whose source MAC address is A with outer VLAN 5. Upon receiving a packet with inner tag VLAN 3 and source MAC address A, the switch tags the packet with outer VLAN 5. Because the port is configured with native VLAN 4, MAC address A is learned by VLAN 4. Upon receiving the reply packet, the switch looks for MAC address A on VLAN 5 because the outer tag of the packet contains VLAN ID 5. However, MAC address A is not learned by VLAN 5, causing floods.

You can configure the Tunnel port to replicate the MAC address of the native VLAN to the outer VLAN to avoid continuous flooding of the packets from the SP network. You can also configure the Tunnel port to replicate the MAC address of the outer VLAN for the outer tag to the native VLAN to avoid continuous flooding of the packets from the customer network.

8.3.5 Layer-2 Transparent Transmission

Working Principle

The Layer-2 transparent transmission feature is designed to realize the transmission of Layer-2 packets between customer networks without impact on SP networks. When a Layer-2 packet from a customer network enters a PE, the PE changes the destination MAC address of the packet to a private address before forwarding the packet. The peer PE changes the destination MAC address to a public address to send the packet to the customer network at the other end, realizing transparent transmission on the SP network.

8.3.6 Priority Replication

Working Principle

If the SP network provides a QoS policy corresponding to a specified User Priority (CoS) in the inner tag, you can replicate the CoS of the inner tag to the outer tag to enable transparent transmission based on the QoS policy provided by the SP network.

8.3.7 Priority Mapping

Working Principle

If the SP network provides various QoS policies corresponding to specified CoS values for different service flows, you can map the CoS value of the inner tag to the CoS value of the outer tag to ensure preferential transmission of service flows based on the QoS policies provided by the SP network.

8.4 Configuration

Configuration	Description and Command	
Configuring QinQ	⚠ Mandatory.	
	switchport mode dot1q-tunnel	Configures a Tunnel port.
	switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }	Adds the VLANs to the Tunnel port in tagged or untagged mode.
	switchport dot1q-tunnel native vlan *VID*	Configures the default VLAN for the Tunnel port.
Configuring C-TAG-Based Selective QinQ	⚠ (Mandatory) It is used to configure C-TAG-based selective QinQ based on basic QinQ. Selective QinQ prevails over basic QinQ.	
	dot1q outer-vid *VID* **register inner-vid** *v_list*	Configures the policy to add the VLAN IDs of outer tags based on inner tags.
Configuring TPIDs	⚠ (Optional) It is used to realize TPID compatibility.	
	frame-tag tpid *tpid*	Configures the TPID of a frame tag. If you want to set it to 0x9100, configure the **frame-tag tpid 9100** command. By default, the TPID is in hexadecimal format. You need to configure this feature on an egress port.
Configuring MAC Address Replication	⚠ (Optional) It is used to configure MAC address replication to prevent floods.	
	mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*	Replicates the dynamic MAC address of the source VLAN to the destination VLAN.
Configuring an Inner/Outer VLAN Tag Modification	⚠ (Optional) It is used to adjust the outer and inner VLAN tags of the packets transmitted over SP networks based on network topologies.	

Configuration	Description and Command	
Policy	**dot1q relay-vid** *VID* **translate local-vid** *v_list*	Configures the policy to change the VLAN IDs of outer tags based on the outer tags.
	dot1q relay-vid *VID* **translate inner-vid** *v_list*	Configures the policy to change the VLAN IDs of outer tags based on inner tags.
	dot1q new-outer-vlan *VID* **translate old-outer-vlan vid inner-vlan** *v_list*	Configures the policy to change the VLAN IDs of outer tags based on outer and inner tags.
Configuring Priority Mapping and Priority Replication	(Optional) It is used to apply the QoS policy provided by the SP network by priority replication.	
	inner-priority-trust enable	Replicates the value of the User Priority field in the inner tag (C-TAG) to the User Priority field of the outer tag (S-TAG).
	(Optional) It is used to apply the QoS policy provided by the SP network by priority mapping.	
	dot1q-Tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*	Sets the value of the User Priority field in the outer tag (S-TAG) based on the User Priority field of the inner tag (C-TAG).
Configuring Layer-2 Transparent Transmission	(Optional) It is used to transmit MSTP and GVRP packets transparently based on the customer network topology without affecting the SP network topology.	
	l2protocol-tunnel stp	Enables STP transparent transmission in global configuration mode.
	l2protocol-tunnel stp enable	Enables STP transparent transmission in interface configuration mode.
	l2protocol-tunnel{**STP**|**GVRP**}**tunnel-dmac** *mac-address*	Configures a transparent transmission address.

Pay attention to the following limitations when you configure QinQ:

Do not configure a routed port as the Tunnel port.

Do not enable 802.1X on the Tunnel port.

Do not enable the port security function on the Tunnel port.

When the Tunnel port is configured as the source port of the remote switched port analyzer (RSPAN), the packets whose outer tags contain VLAN IDs consistent with the RSPAN VLAN IDs are monitored.

If you want to match the ACL applied to the Tunnel port with the VLAN IDs of inner tags, use the inner keyword.

⚠ Configure the egress port of the customer network connected to the SP network as an Uplink port. If you configure the TPID of the outer tag on a QinQ-enabled port, set the TPID of the outer tag on the Uplink port to the same value.

⚠ By default, the maximum transmission unit (MTU) on a port is 1,500 bytes. After added with an outer VLAN tag, a packet is four bytes longer. It is recommended to increase the port MTU on the SP networks to at least 1,504 bytes.

⚠ After a switch port is enabled with QinQ, you must enable SVGL sharing before enabling IGMP snooping. Otherwise, IGMP snooping will not work on the QinQ-enabled port.

⚠ If a packet matches two or more ACL-based selective QinQ policies without priority, only one policy is executed. It is recommended to specify the priority.

8.4.1 Configuring QinQ

Configuration Effect

- Implement Layer-2 VPN based on a port-based QinQ policy.

Notes

- It is not recommended to configure the native VLAN of the Trunk port on the PE as its default VLAN, because the Trunk port strips off the tags containing the native VLAN IDs when sending packets.

Configuration Steps

↘ Configuring the Tunnel port

- (Mandatory) Configure the Tunnel port in interface configuration mode.
- Run the **switchport mode dot1q-tunnel** command in interface configuration mode to configure the Tunnel port.

Command	switchport mode dot1q-tunnel
Parameter Description	N/A
Defaults	By default, no Tunnel port is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

↘ Configuring the Native VLAN

- Mandatory.
- Configure the native VLAN for the Tunnel port.
- After you configure the native VLAN, add it to the VLAN list of the Tunnel port in untagged mode.
- Run the **switchport dot1q-tunnel native vlan** *VID* command in interface configuration mode to configure the default VLAN for the Tunnel port.
- If the native VLAN is added to the VLAN list in untagged mode, the outgoing packets on the Tunnel port are not tagged. If the native VLAN is added to the VLAN list in tagged mode, the outgoing packets on the Tunnel port are tagged with

the native VLAN ID. To ensure the uplink and downlink transmission, add the native VLAN to the VLAN list in untagged mode.

Command	**switchport dot1q-tunnel native vlan** *VID*
Parameter Description	*VID*: Indicates the ID of the native VLAN. The value ranges from 1 to 4,094. The default value is 1.
Defaults	By default, the native VLAN is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure the VLAN of the SP network.

Adding the VLANs on the Tunnel port

- Mandatory.
- After you configure the native VLAN, add it to the VLAN list of the Tunnel port in untagged mode.
- If port-based QinQ is enabled, you do not need to add the VLANs of the customer network to the VLAN list of the Tunnel port.
- If selective QinQ is enabled, add the VLANs of the customer network to the VLAN list of the Tunnel port in tagged or untagged mode based on requirements.
- Run the **switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* } command in interface configuration mode to add VLANs to the VLAN list of the Tunnel port. Upon receiving packets from corresponding VLANs, the Tunnel port adds or removes tags based on the settings.

Command	**switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist*	[**add**] **untagged** *vlist*	**remove** *vlist* }
Parameter Description	*v_list*: Indicates the list of the VLANs on the Tunnel port.
Defaults	By default, VLAN 1 is added to the VLAN list of the Tunnel port in untagged mode. Other VLANs are not added.
Command Mode	Interface configuration mode
Usage Guide	Use this command to add or remove VLANs on the Tunnel port and specify whether the outgoing packets are tagged or untagged. If basic QinQ is enabled, add the native VLAN to the VLAN list of the Tunnel port in untagged mode.

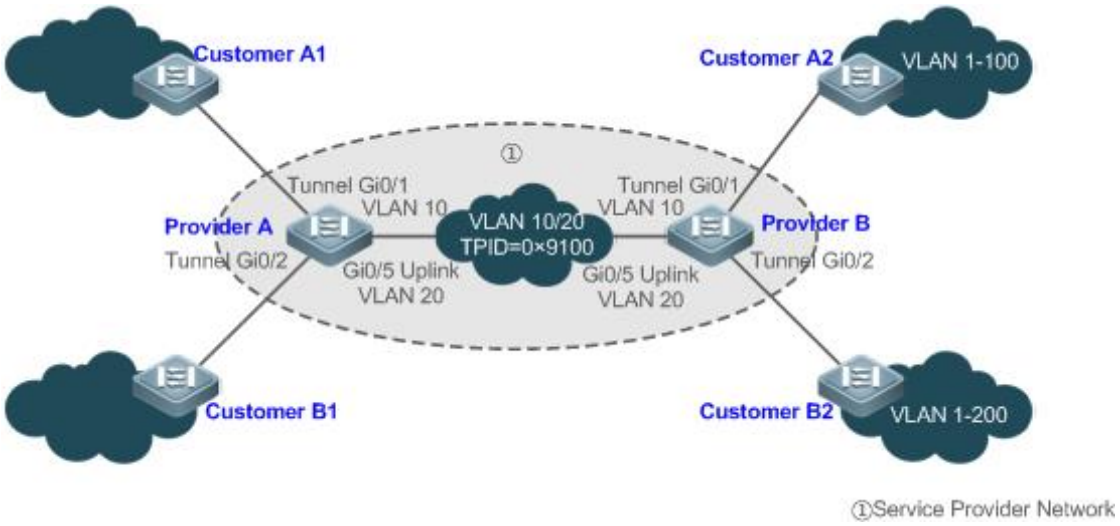
Verification

Check the Tunnel port configuration.

- Check whether the Tunnel port is configured properly on a switch.

Configuration Example

Configuring Basic QinQ to Implement Layer-2 VPN

Scenario **Figure 8-7**	
Configuration Steps	● Configure Tunnel ports on the PEs and connect the CEs to the Tunnel ports. ● Configure the native VLANs for the Tunnel ports and add the native VLANs to the VLAN lists of the Tunnel ports respectively in untagged mode. ● Configure VLANs on the customer networks based on requirements. QinQ-enabled switches encapsulate outer tags in packets for transmission over the SP network. Therefore, you do not need to configure customer VLANs on the PEs. The TPID is 0x8100 by default according to IEEE802.1Q. On some third-party switches, the TPID is set to a different value. If such switches are deployed, set the TPIDs on the ports connected to the third-party switches to realize TPID compatibility. If the PEs are connected through Trunk ports or Hybrid ports, do not configure the native VLANs for the Trunk ports or Hybrid ports as the default VLANs for the Tunnel ports. The Trunk ports or Hybrid ports strip off the VLAN tags containing the Native VLAN IDs when sending packets.

Provider A	Step 1: Create VLAN 10 and VLAN 20 on the SP network to segregate the data of Customer A and Customer B.
	`ProviderA#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`ProviderA(config)#vlan 10`
	`ProviderA(config-vlan)#exit`
	`ProviderA(config)#vlan 20`
	`ProviderA(config-vlan)#exit`
	Step 2: Enable basic QinQ on the port connected to the network of Customer A to use VLAN 10 for tunneling.
	`ProviderA(config)#interface gigabitEthernet 0/1`
	`ProviderA(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel`
	`ProviderA(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 10`

	ProviderA(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 10 Step 3: Enable basic QinQ on the port connected to the network of Customer B to use VLAN 20 for tunneling. ProviderA(config)#interface gigabitEthernet 0/2 ProviderA(config-if-GigabitEthernet 0/2)#switchport mode dot1q-tunnel ProviderA(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel native vlan 20 ProviderA(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel allowed vlan add untagged 20 Step 4: Configure an Uplink port. ProviderA(config)# interface gigabitEthernet 0/5 ProviderA(config-if-GigabitEthernet 0/5)#switchport mode uplink Step 5: Change the TPID of the outgoing packets on the Uplink port to a value (for example, 0x9100) recognizable by third-party switches. ProviderA(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100 Step 6: Configure Provider B by performing the same steps.
Verification	Customer A1 sends a packet containing VLAN ID 100 destined to Customer A2. The packet through Provider A is tagged with the outer tag specified by the Tunnel port. The packet that reaches Customer A2 carries the original VLAN ID 100. Check whether the Tunnel port is configured correctly. Check whether the TPID is configured correctly.
Provider A	ProviderA#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 10 switchport dot1q-tunnel native vlan 10 spanning-tree bpdufilter enable ! interface GigabitEthernet 0/2 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 20 switchport dot1q-tunnel native vlan 20 spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5

	switchport mode uplink frame-tag tpid 0x9100 ProviderA#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: ProviderA#show frame-tag tpid Ports Tpid ------- ------------ Gi0/5 0x9100
Provider B	Check Provider B by performing the same steps.

Common Errors

- The native VLAN is not added to the VLAN list of the Tunnel port in untagged mode.
- No TPID is configured on the port connected to the third-party switch on which TPID is not 0x8100. As a result, packets cannot be recognized by the third-party switch.

8.4.2 Configuring C-TAG-Based Selective QinQ

Configuration Effect

- 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.

Notes

- C-TAG-based selective QinQ must be configured based on basic QinQ.
- Some selective QinQ policies are not supported on some products due to limitations of chips.
- If you need to continue to adopt the VLAN tag priority specified by the customer 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 need to configure priority replication to set the CoS of the outer tag to the specified value.

Configuration Steps

Configuring a Policy to Add the VLAN IDs of Outer Tags Based on Inner Tags

- Mandatory.
- Upon receiving a packet, the Tunnel port adds the VLAN ID of the outer tag based on the VLAN ID of the inner tag. This function enables the Tunnel port to add the VLAN ID of the inner tag to the outer tag and adds the port to the VLAN in untagged mode. In this way, the outgoing packets carry the original inner tags.

The ACL-based QinQ policy prevails over the port-based and C-TAG-based QinQ policy.

When a member port is added to or removed from an aggregate port (AP), the QinQ policy configured on the AP port will be deleted. You need to configure the policy again. It is recommended that you configure a selective QinQ policy on the AP port after you configure its member ports.

You must configure the Tunnel port and the port connected to the public network to permit packets with specified VLAN IDs (including the native VLAN ID) in the outer tag to pass through.

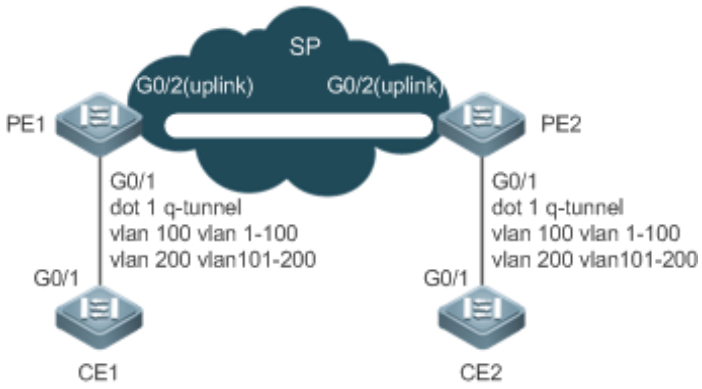
Command	**dot1q outer-vid** *VID* **register inner-vid** *v_list*
Parameter Description	N/A
Defaults	By default, no policy is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Check whether the users within the VLANs can communicate with each other.
- Check whether Layer-2 VPN is implemented.
- Check whether different service traffic is transmitted based on the selective QinQ policy, such as outer tag insertion, priority replication, and priority mapping.

Configuration Example

Implementing Layer-2 VPN and Service Flow Management Through C-TAG-Based Selective QinQ

Scenario **Figure 8-8**	
Configuration Steps	● Configure the ports on PE 1 and PE 2 connected to CE 1 and CE 2 as Tunnel ports. ● Configure a selective QinQ policy to add an outer tag to the packet based on its inner tag. ● If the SP network provides a VLAN-based QoS policy, the policy enables the port to add the outer tags with the corresponding VLAN ID to the specified service flow packets. ● If the SP network provides a CoS-based QoS policy and the CoS value is the same as that of the inner tag, you can configure priority mapping to replicate the CoS value of the inner tag to the outer VLAN tag so that the packet is transmitted based on the priority policy for the inner tag. ● If the SP network provides a CoS-based QoS policy, you can configure priority mapping to set the CoS value of the outer VLAN tag to a specified value so that the packet is transmitted based on the priority policy.

PE1	Step 1: Configure the VLAN for transparent transmission.
	`PE1#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`PE1(config)#vlan 100`
	`PE1(config-vlan)#exit`
	`PE1(config)#vlan 200`
	`PE1(config-vlan)#exit`
	Step 2: On the Downlink port of the access switch, configure a selective QinQ policy to add outer tags based on inner tags.
	Configure port Gi 0/1 as a Tunnel port.
	`PE1(config)#interface gigabitEthernet 0/1`
	`PE1(config-if)# switchport mode dot1q-tunnel`
	Add VLAN 101 and VLAN 201 of the SP to the VLAN list of the Tunnel port and configure the Tunnel port to strip off the outer tag from incoming packets.
	`PE1(config-if)# switchport dot1q-tunnel allowed vlan add untagged 100,200`
	Configure the Tunnel port to add outer tag VLAN 100 to incoming data frames containing inner tag VLAN 1–

	100.
	`PE1(config-if)# dot1q outer-vid 100 register inner-vid 1-100`
	Configure the Tunnel port to add outer tag VLAN 200 to incoming data frames containing inner tag VLAN 101-200.
	`PE1(config-if)# dot1q outer-vid 200 register inner-vid 101-200`
	Step 3: Configure the port that accesses the SP network as an Uplink port.
	`PE1(config)# interface gigabitEthernet 0/2`
	`PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink`

PE2	● Perform the same configuration on PE 2.
Verification	Verify the configuration by checking whether: ● The Downlink port is configured as a Tunnel port. ● The VLAN specified by the outer tag is added to the VLAN list of the Tunnel port. ● The selective QinQ policy on the Tunnel port is correct. ● The Uplink port is configured correctly. Step 1: Check whether the VLAN mapping policy is correct.

PE1	`PE1#show running-config interface gigabitEthernet 0/1`
	`interface GigabitEthernet 0/1`
	` switchport mode dot1q-tunnel`
	` switchport dot1q-tunnel allowed vlan add untagged 100,200`
	` dot1q outer-vid 100 register inner-vid 1-200`
	` dot1q outer-vid 200 register inner-vid 101-200`
	` spanning-tree bpdufilter enable`
	`!`
	Step 2: Check the C-TAG-based selective QinQ policy. Check whether the mapping relationship between the inner and outer VLAN tags is correct.
	`PE1#show registration-table`
	
	`Ports Type Outer-VID Inner-VID-list`
	`------ ---------- ---------- --------------`
	`Gi0/1 Add-outer 100 1-200`
	`Gi0/1 Add-outer 200 101-200`

8.4.3 Configuring TPIDs

Configuration Effect

Configure the TPIDs in the tags on SP network devices to realize TPID compatibility.

Notes

If a PE connected to a third-party switch on which the TPID is not 0x8100, you need to configure the TPID on the port of the PE connected to the third-party switch.

⚠ Do not set the TPIDs to any of the following values: 0x0806 (ARP), 0x0200 (PUP), 0x8035 (RARP), 0x0800 (IP), 0x86DD (IPv6), 0x8863/0x8864 (PPPoE), 0x8137 (IPX/SPX), 0x8000 (IS-IS), 0x8809 (LACP), 0x888E (802.1X), 0x88A7 (clusters), and 0x0789 (reserved by our company).

Configuration Steps

- If a PE connected to a third-party switch on which the TPID is not 0x8100, you need to configure the TPID on the port of the PE connected to the third-party switch.
- TPIDs can be configured in interface configuration mode and global configuration mode. The following example adopts interface configuration mode.

Configure the **frame-tag tpid** *0x9100* command in interface configuration mode to change the TPID to 0x9100. For details about the TPID value, see section 1.4.5.

Command	**frame-tag tpid** *tpid*
Parameter Description	*tpid:* Indicates the new value of the TPID.
Defaults	The default value of the TPID is 0x8100.
Command Mode	Interface configuration mode
Usage Guide	If a PE is connected to a third-party switch on which the TPID is not 0x8100, use this command to configure the TPID on the port connected to the third-party switch.

Verification

Check whether the TPID is configured.

Configuration Example

↘ Configuring the TPID on a port

Configuration Steps	Configure the TPID on a port.
	`Hostname(config)# interface gigabitethernet 0/1`
	`Hostname(config-if)# frame-tag tpid 9100`

Verification	Displaythe TPID on the port.
	`Hostname# show frame-tag tpid interfaces gigabitethernet 0/1`
	`Port tpid`
	`------- -------------`
	`Gi0/1 0x9100`

8.4.4 Configuring MAC Address Replication

Configuration Effect

- Replicate the dynamic address learned on a port from one VLAN to another.
- Avoid packet floods when service flows are segregated through MAC-based ACLs.

Notes

After MAC address replication is disabled, the system will delete all the learned MAC address entries from the destination VLAN.

MAC address replication can be configured on a port only once. If you need to modify the configuration, delete the current configuration and configure it again.

VLAN MAC address replication cannot be used together with VLAN sharing, and the MAC addresses cannot be replicated to dynamic VLANs.

Up to eight destination VLANs can be configured on each port. MAC address replication takes effect even if the port does not belong to the specified destination VLAN.

MAC address replication cannot be configured on the Host and Promiscuous ports, monitoring ports, and port security-/802.1X-enabled ports.

Only dynamic addresses can be replicated. 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.

Hot backup is not supported. After primary/secondary switchover occurs, it is recommended that you disable MAC address replication and then enable it again.

The MAC address entries obtained through MAC address replication cannot be deleted manually. If you need to delete these entries, disable MAC address replication.

Configuration Steps

Configuring MAC Address Replication

- Perform this configuration to replicate MAC addresses from one VLAN to another to avoid packet floods.

- Run the **mac-address-mapping** <1-8> **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id* command on a Trunk port to enable MAC address replication. *src-vlan-list* and *dst-vlan-id* specify the VLAN range.

Command	**mac-address-mapping** *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*
Parameter Description	*x:* Indicates the index number for MAC address replication. The value ranges from 1 to 8. *src-vlan-list*: Indicates the source VLAN list. *dst-vlan-id:* Indicates the destination VLAN list.
Defaults	By default, MAC address replication is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Check whether the MAC address of the specified VLAN is replicated to another VLAN.

Configuration Example

Configuring MAC Address Replication

Configuration Steps	• Configure MAC address replication.
	`Hostname(config)# interface gigabitethernet 0/1`
	`Hostname(config-if)# switchport mode trunk`
	`Hostname(config-if)#mac-address-mapping 1 source-vlan 1-3 destination-vlan 5`

Verification	• Check whether the configuration takes effect on the port.
	• Send a packet from the source VLAN and check whether the source MAC address of the packet is replicated to the destination VLAN.
	`Hostname# show interfaces mac-address-mapping`
	`Ports destination-VID Source-VID-list`
	`----------`
	`Gi0/1 5 1-3`

Common Errors

- See "Notes".

8.4.5 Configuring Priority Mapping and Priority Replication

Configuration Effect

- If an SP network provides a QoS policy based on the User Priority field of the inner tag, configure priority replication to apply the QoS policy to the outer tag.
- If an SP network provides a QoS policy based on the User Priority field of the inner tag, configure priority mapping to apply the User Priority field provided by the SP network to the outer tag.

Notes

⚠ Only a Tunnel port can be configured with priority replication, which has a higher priority than trusted QoS but lower than ACL-based QoS.

⚠ Priority replication and priority mapping cannot be both enabled on one port.

⚠ Only a Tunnel port can be configured with priority mapping, which prevails over QoS.

⚠ The configuration of priority mapping does not take effect if no trust mode is configured (trust none) or the trust mode is not matched with priority mapping.

Configuration Steps

- Only a Tunnel port can be configured with priority mapping or priority replication.
- Configure priority replication to apply the inner tag-based QoS policy provided by the SP network.
- Configure priority mapping to configure the User Priority field of the outer VLAN tag based on the inner tag and apply the QoS policy flexibly.
- To enable priority replication, run the **inner-priority-trust enable** command on the Tunnel port.
- To enable priority mapping, run the **dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value* command on the Tunnel port.

inner-cos-value and *outer-cos-value* range from 0 to 7.

ℹ The following priority mapping is used when no priority mapping is configured:

inner pri	0	1	2	3	4	5	6	7
outer pri	0	1	2	3	4	5	6	7

Command	**inner-priority-trust enable**
Parameter Description	N/A
Defaults	By default, priority replication is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

Command	**dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value*
Parameter Description	*inner-cos-value*: Indicates the CoS value of the inner tag. *outer-cos-value*: Indicates the CoS value of the outer tag.
Defaults	By default, priority mapping is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Run the **show inner-priority-trust interfaces** *type intf-id* command and the **show interfaces** *type intf-id* **remark** command to check whether priority mapping or priority replication takes effect.

Configuration Example

Configuring Priority Mapping and Priority Replication

Configuration Steps	• To maintain the packet priority, you need to replicate the priority of the inner tag in a packet to the outer tag on the Tunnel port.
	• To flexibly control the packet priority on the Tunnel port, you can add outer tags of different priorities to packets based on the priorities of the inner tags in the packets.
	Configure priority replication.
	`Hostname(config)# interface gigabitethernet 0/1`
	`Hostname(config-if)#mls qos trust cos`
	`Hostname(config-if)# inner-priority-trust enable`
	`Hostname(config)# end`
	Configure priority mapping.
	`Hostname(config)# interface gigabitethernet 0/2`
	`Hostname(config-if)#dot1q-Tunnel cos 3 remark-cos 5`

Verification	• Display the priority configuration on the port.
	Check whether priority replication is enabled on the Tunnel port.
	`Hostname# show inner-priority-trust interfaces gigabitethernet 0/1`
	`Port inner-priority-trust`
	`------ ------------------`
	`Gi0/1 enable`
	Display the priority mapping configured on the Tunnel port.
	`Hostname# show interfaces gigabitethernet 0/1 remark`
	`Ports Type From value To value`
	`---------- ---------- ---------- --------`
	`Gi0/1 Cos-To-Cos 3 5`

Common Errors

See "Notes".

8.4.6 Configuring Layer-2 Transparent Transmission

Configuration Effect

Transmit Layer-2 packets transparently without impact on the SP network and the customer network.

Notes

- If STP is not enabled, you need to run the **bridge-frame forwarding protocol bpdu** command to enable STP transparent transmission.
- Transparent transmission enabled on a port takes effect only after enabled globally. When transparent transmission takes effect on the port, the port does not participate in related protocol calculation. If the port receives a packet whose destination MAC address is the special broadcast address, it determines that a networking error occurs and discards the packet.

Configuration Steps

Configuring STP Transparent Transmission

- Mandatory if you need to transparently transmit BPDU packets through STP.
- Enable STP transparent transmission in global configuration mode and interface configuration mode.
- Run the **l2protocol-tunnel stp** command in global configuration mode to enable STP transparent transmission.
- Run the **l2protocol-tunnel stp enable** command in interface configuration mode to enable STP transparent transmission.

Command	**l2protocol-tunnel stp**
Parameter Description	N/A
Defaults	By default, STP transparent transmission is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**l2protocol-tunnel stp enable**
Parameter Description	N/A
Defaults	By default, STP transparent transmission is disabled.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Transparent Transmission Address

- Optional.
- Configure a transparent transmission address.

Command	**l2protocol-tunnel stp tunnel-dmac** *mac-address*

Parameter Description	*mac-address*: Indicates the address used to transparently transmit packets.
Defaults	By default, the first three bytes of the transparent transmission address is 01d0f8, and the last three bytes are 000005 and 000006 for STP and GVTP respectively.
Command Mode	Global configuration mode
Usage Guide	The following addresses are available for STP: 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2. The following addresses are available for GVRP: 01d0.f800.0006 and 011a.a900.0006. When no transparent transmission address is configured, the default settings are used.

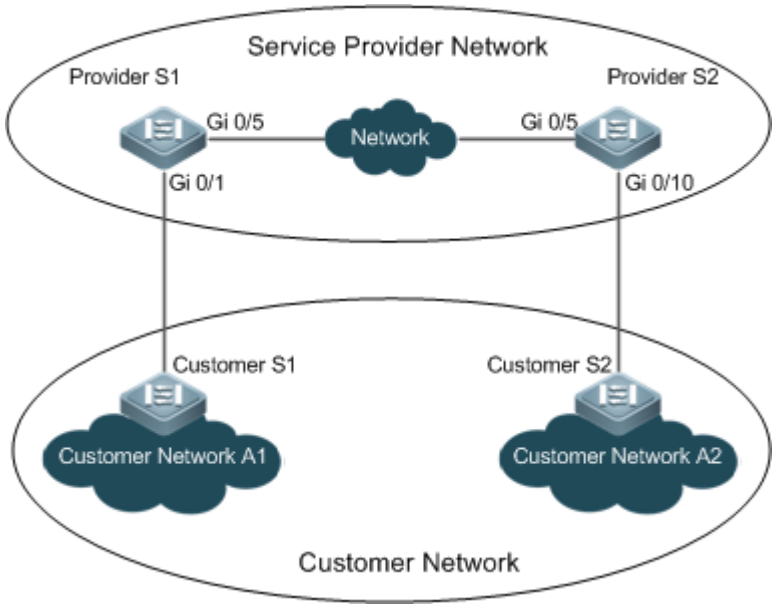
Verification

Run the **show l2protocol-tunnel stp** command to check whether the transparent transmission address is configured correctly.

Configuration Example

The following example shows how to configure STP transparent transmission.

Configuring STP Transparent Transmission

Scenario Figure 8-9	
Configuration Steps	● On the PEs (Provider S1 and Provider S2), enable STP transparent transmission in global configuration mode and interface configuration mode. ● Before you enable STP transparent transmission, enable STP in global configuration mode to allow the switches to forward STP packets.
Provider S1	Step 1: Enable STP. `bridge-frame forwarding protocol bpdu` Step 2: Configure the VLAN for transparent transmission.

	ProviderS1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. ProviderS1(config)#vlan 200 ProviderS1(config-vlan)#exit Step 3: Enable basic QinQ on the port connected to the customer network and use VLAN 200 for tunneling. ProviderS1(config)#interface gigabitEthernet 0/1 ProviderS1(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel ProviderS1(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 Step 4: Enable STP transparent transmission on the port connected to the customer network. ProviderS1(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable ProviderS1(config-if-GigabitEthernet 0/1)#exit Step 5: Enable STP transparent transmission in global configuration mode. ProviderS1(config)#l2protocol-tunnel stp Step 4: Configure an Uplink port. ProviderS1(config)# interface gigabitEthernet 0/5 ProviderS1(config-if-GigabitEthernet 0/5)#switchport mode uplink
Provider S2	Configure Provider S2 by performing the same steps.
Verification	Step 1: Check whether STP transparent transmission is enabled in global configuration mode and interface configuration mode. ProviderS1#show l2protocol-tunnel stp L2protocol-tunnel: Stp Enable GigabitEthernet 0/1 l2protocol-tunnel stp enable Step 2: Verify the configuration by checking whether: ● The port type is dot1q-tunnel. ● The outer tag VLAN is consistent with the native VLAN and added to the VLAN list of the Tunnel port. ● The port that accesses the SP network is configured as an Uplink port. ProviderS1#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 200 switchport dot1q-tunnel native vlan 200

	l2protocol-tunnel stp enable spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink

Common Errors

- STP is not enabled in global configuration mode.
- Transparent transmission is not enabled in global configuration mode and interface configuration mode.

8.5 Monitoring

Displaying

Description	Command
Displays whether the specified port is a Tunnel port.	**show dot1q-tunnel** [**interfaces** *intf-id*]
Displays the configuration of the Tunnel port.	**show interfaces dot1q-tunnel**
Displays the C-TAG-based selective QinQ policies on the Tunnel port.	**show registration-table** [**interfaces** *intf-id*]
Displays the C-TAG-based selective QinQ policies on the Access port, Trunk port or Hybrid port.	**show translation-table** [**interfaces** *intf-id*]
Displays VLAN mapping on ports.	**show interfaces** [*intf-id*] **vlan-mapping**
Displays the TPID configuration on ports.	**show frame-tag tpid interfaces** [*intf-id*]
Displays the configuration of priority replication.	**show inner-priority-trust**
Displays the configuration of priority mapping.	**show interface intf-name remark**
Displays the configuration of MAC address replication.	**show mac-address-mapping**
Displays the configuration of Layer-2 transparent transmission.	**show l2protocol-tunnel** { **gvrp** | **stp** }

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs QinQ.	**debug bridge qinq**

9 Configuring ERPS

9.1 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 designed for Ethernet rings. ERPS prevents broadcast storms caused by data loops in an idle Ethernet ring and can rapidly recover the communication between nodes in the event that a link is disconnected in the Ethernet ring.

The Spanning Tree Protocol (STP) is another technique used to solve the Layer-2 loop problem. STP is at the mature application stage but requires a relatively long (seconds) convergence time compared to ERPS. ERPS reaches a Layer-2 convergence speed of less than 50 ms, faster than that of STP.

Scenario

- ITU-T G.8032/Y.1344: Ethernet ring protection switching

9.2 Applications

Application	Description
Single-Ring Protection	Only one ring exists in a network topology.
Tangent-Ring Protection	Two rings in a network topology share one device.
Intersecting-Ring Protection	Two or more rings in a network topology share one link.

9.2.1 Single-Ring Protection

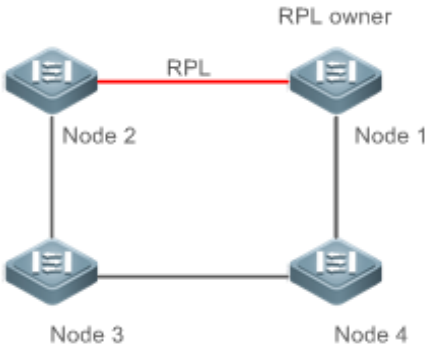
Scenario

Only one ring in a network topology needs to be protected.

In Figure 9-1, the network topology has only one ring, only one ring protection link (RPL) owner node, and only one RPL. All nodes must belong to the same ring automatic protection switching (R-APS) virtual local area network (VLAN).

- All devices in the ring network must support ERPS.
- Each link between devices must be a direct link without any intermediate device.

Figure 9-1



Remarks	The four devices in the ring network are aggregation switches.

Deployment

- All nodes in the physical topology are connected in ring mode.
- ERPS blocks the RPL to prevent loops. In Figure 9-1, the link between Node 1 and Node 2 is an RPL.
- ERPS is used to detect failures on each link between adjacent nodes.

9.2.2 Tangent-Ring Protection

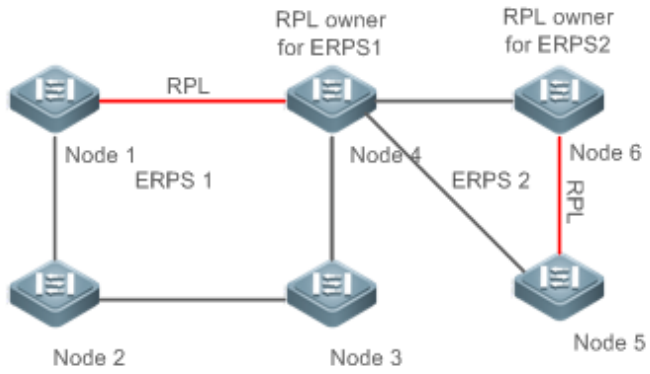
Scenario

The two rings in a network topology that share one device need to be protected.

In Figure 9-2, the two rings in the network topology share one device. Each ring has only one PRL owner node and only one RPL. The two 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.

Figure 9-2



Remarks	The devices in the ring network are aggregation switches.

Deployment

- All nodes in the physical topology are connected in ring mode.
- ERPS blocks the RPL of each ring to prevent loops.
- ERPS is used to detect failures on each link between adjacent nodes.

9.2.3 Intersecting-Ring Protection

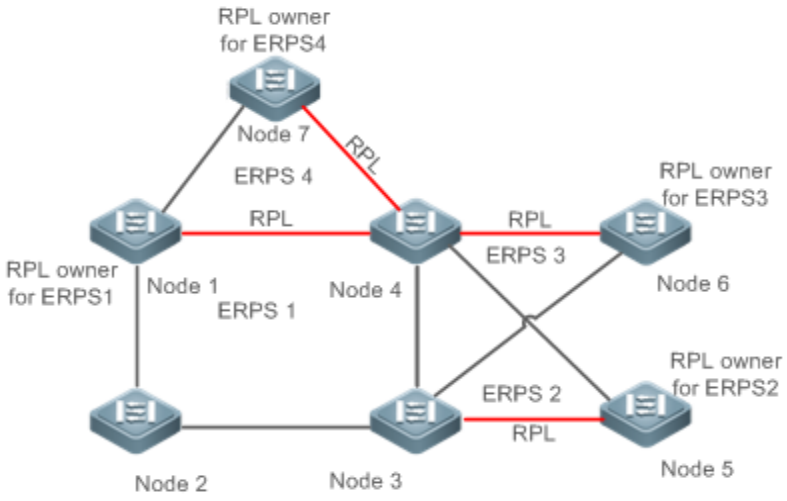
Scenario

Two or more rings in a network topology share one link. (Each link between intersecting nodes must be a direct link without any intermediate node.)

In Figure 9-3, four rings exist in the network topology. Each ring has only one PRL owner node and only one RPL. The four 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.

Figure 9-3



Remarks	The devices in the ring network are aggregation switches.

Deployment

- All nodes in the physical topology are connected in ring mode.
- ERPS blocks the RPL of each ring to prevent loops.
- ERPS is used to detect failures on each link between adjacent nodes.

9.3 Features

Basic Concepts

Ethernet Ring

Ethernet rings are classified into common Ethernet rings and Ethernet subrings.

- **Common Ethernet ring:** Is an Ethernet topology with ring connection.
- **Ethernet subring:** An open topology that is mounted on other rings or networks through intersecting nodes and forms a closed topology with the channel between the intersecting nodes belonging to other rings or networks.

An Ethernet ring (a common Ethernet ring or an Ethernet subring) can be in one of the following states:

- **Idle state:** The physical links in the entire ring network are reachable.
- **Protection state:** A physical link in the ring network is disconnected.

Link and Channel

- **RPL:** An Ethernet ring (a common Ethernet ring or an Ethernet subring) has only one RPL. When an Ethernet ring is idle, the RPL is blocked and does not forward data packets to prevent loops. In Figure 9-2, the link between Node 1 and Node 4 is the RPL of ERPS 1, and Node 4 blocks the RPL port (the port mapped to the RPL). The link between Node 4 and Node 5 is the RPL of ERPS 2, and Node 5 blocks the RPL port.
- **Subring link:** Belongs to a subring in intersecting rings and is controlled by the subring. In Figure 9-3, ERPS 1 is a common Ethernet ring, and ERPS 2 is an Ethernet subring. The link between Node 4 and Node 5 and the link between Node 3 and Node 5 belong to ERPS 2. The other links belong to ERPS 1.

The link between Node 3 and Node 4 belongs to ERPS 1 rather than ERPS 2, and the link is not controlled by ERPS 2.

- **R-APS virtual channel:** Transmits ERPS packets of subrings between intersecting nodes in intersecting rings, but it does not belong to the subring. In Figure 9-3, Node 1 blocks the RPL, and the packets of subring ERPS 2 are transmitted through the direct link between Node 3 and Node 4 in Ethernet ring ERPS 1. The direct link between Node 3 and Node 4 is the R-APS virtual channel of ERPS 2.

Node

Each device in an Ethernet ring is a node.

ERPS has the following node roles for a specific Ethernet ring:

- **RPL owner node:** 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. An Ethernet ring (a common Ethernet ring or an Ethernet subring) has only one RPL owner node. In Figure 9-2, Node 1 functions as the RPL owner node of Ethernet ring ERPS 1, and Node 6 functions as the RPL owner node of Ethernet subring ERPS 2.
- **Non-RPL owner node:** Any other node than the RPL owner node in an Ethernet ring. In Figure 9-2, nodes except Node 1 and Node 6 are non-RPL owner nodes of their respective rings.

ERPS has the following roles globally (not for a specific Ethernet ring):

- **Intersecting node:** A node that belongs to multiple intersecting Ethernet rings. In Figure 9-3, Node 3 and Node 4 are intersecting nodes.
- **Non-intersecting node:** A node that belongs to only one intersecting Ethernet ring. In Figure 9-3, Node 2 is a non-intersecting node.

VLAN

ERPS supports two types of VLAN: R-APS VLAN and data VLAN.

- **R-APS VLAN:** A VLAN for transmitting ERPS packets. On a device, the ports accessing an ERPS ring belong to the R-APS VLAN, and only such ports can join the R-APS VLAN. R-APS VLANs of different ERPS rings must be different. IP address configuration is prohibited on the R-APS VLAN ports.
- **Data VLAN:** A VLAN for transmitting data packets. Both ERPS ports and non-ERPS ports can be assigned to a data VLAN.

R-APS VLANs of different ERPS rings must be configured differently to differentiate packets of different ERPS rings; otherwise, ERPS may be abnormal.

ERPS Packet

ERPS packets (also called R-APS packets) are classified into Signal Fail (SF) packets, No Request (NR) packets, No Request, RPL Blocked (NR, RB) packets, and flush packets.

- SF packet: When the link of a node is down, the node sends SF packets 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.
- (RR, RB) packet: When all nodes in an ERPS ring function properly, the RPL owner node sends (RR, RB) packets periodically.
- Flush packet: In an intersecting ring, 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.

ERPS Timer

ERPS timers include the Holdoff timer, Guard timer, and WTR timer.

- **Holdoff 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:** Is used to prevent a device from receiving expired R-APS messages. When the device detects that a link failure is cleared, it sends link recovery packets and starts the Guard timer. During the period before timer expiration, all packets except flush packets indicating a subring topology change will be discarded.
- **Wait-to-restore (WTR) timer:** Is effective only for RPL owner devices to avoid ring status misjudgment. When an RPL owner device detects that a failure is cleared, it does 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 timer expiration, the RPL owner device cancels the timer and does not perform topology switching.

Overview

Feature	Description
Ring Protection	Prevents broadcast storms caused by data loops and can rapidly recover the communication between nodes in the event that a link is disconnected in the Ethernet ring.
Load Balancing	Configures multiple Ethernet subrings in one ring network and forwards the traffic of different VLANs through different Ethernet subrings to balance load.

9.3.1 Ring Protection

Ring protection prevents broadcast storms caused by data loops and can rapidly recover the communication between nodes in the event that a link is disconnected in the Ethernet ring.

Working Principle

Normal Status

- All nodes in the physical topology are connected in ring mode.
- ERPS blocks the RPL to prevent loops.
- ERPS is used to detect failures on each link between adjacent nodes.

Link Failure

- A node adjacent to a failed node detects the failure.
- The nodes adjacent to a failed link block the failed link and send SF packets to notify other nodes in the same ring.
- The R-APS (SF) packet triggers the RPL owner node to unblock the RPL port. All nodes update their MAC address entries and ARP/ND entries and the ring enters the protection state.

Link Recovery

- When a failed link is restored, adjacent nodes still block the link and send NR packets indicating that no local failure exists.
- When the RPL owner node receives the first R-APS (NR) packet, it starts the WTR timer.
- When the timer times out, the RPL owner node blocks the RPL and sends an (NR, RB) packet.
- After receiving the (NR, RB) packet, other nodes update their MAC address entries and ARP/ND entries, and the node that sends the NR packet stops periodic packet transmission and unblocks the port.
- The ring network is restored to the normal state.

Related Configuration

Configuring the R-APS VLAN

By default, no R-APS VLAN is configured.

Run the **erps raps-vlan** command to configure the R-APS VLAN (management VLAN) of an ERPS ring to transmit ERPS packets.

Configuring an ERPS Ring

Run the **rpl-port** command in R-APS VLAN mode to configure the ERPS ring mapped to an R-APS VLAN.

Configuring an RPL and an RPL Owner Node

Run the **rpl-port** command in R-APS VLAN mode to specify an RPL and an RPL owner node.

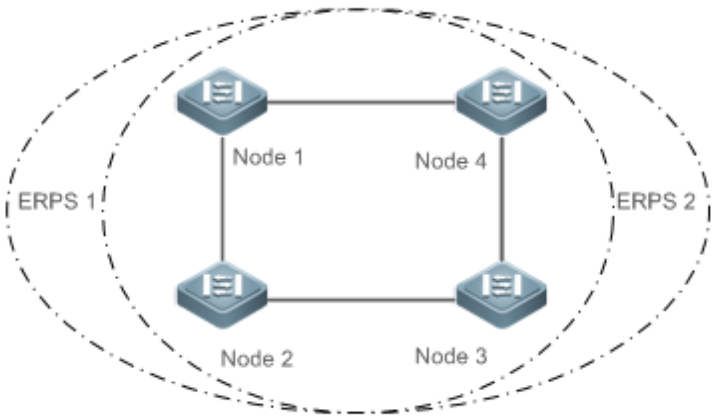
9.3.2 Load Balancing

You can configure multiple Ethernet subrings in one physical ring network and forward the traffic of different VLANs through different Ethernet subrings to balance load.

Working Principle

The multiple VLANs in a ring network can have their respective traffic forwarded by different paths through ERPS to balance load.

Figure 9-4 Single-Ring Load Balancing



In a physical ring network, multiple Ethernet rings can be configured to forward traffic of different VLANs (called protected VLANs) by different topologies to realize load balancing.

In Figure 9-4, two Ethernet rings are configured with different protected VLANs in the physical ring network. Node 1 is the RPL owner node of ERPS 1 and Node 3 is RPL owner node of ERPS 2. With such configurations, data of different VLANs can be transmitted by different links to realize single-ring load balancing.

Related Configuration

Configuring the Protected VLAN of an Ethernet Ring

Run the **protected-instance** command in R-APS VLAN mode to configure a protected VLAN set to realize load balancing.

9.4 Configuration

Configuration	Description and Command	
Single-Ring Configuration (Basic Function)	(Mandatory) Perform this configuration in global configuration mode.	
	erps enable	Enables ERPS.
	erps raps-vlan	Configures the R-APS VLAN of an Ethernet ring.
	(Mandatory) Perform this configuration in R-APS VLAN mode.	
	ring-port	Configures an ERPS ring.
	rpl-port	Configures the RPL owner node.
	state enable	Enables the specified R-APS ring.
Tangent-Ring Configuration	Tangent-ring configuration is based on single-ring configuration.	
Intersecting-Ring Configuration	(Optional) Perform this configuration in R-APS VLAN mode based on single-ring configuration.	
	associate sub-ring raps-vlan	Associates Ethernet subrings.
	sub-ring tc-propagation enable	Enables subring topology change notification.
Load Balancing Configuration	(Optional) Perform this configuration in R-APS VLAN mode based on single-ring configuration.	
	protected-instance	Configures the protected VLAN of an Ethernet ring.
ERPS Configuration Modification	(Optional) Perform this configuration in R-APS VLAN mode based on single-ring configuration.	
	timer	Modifies timer parameters.

9.4.1 Single-Ring Configuration (Basic Function)

Configuration Effect

- The single-ring scenario is the basic scenario of ERPS.
- Build an ERPS single-ring topology to realize data link redundancy.
- In an ERPS ring network, quickly switch services from a failed link to a normal link.

Notes

- Only one RPL owner node and only one RPL can be configured in one ERPS ring.
- All nodes in one ERPS ring must belong to the same R-APS VLAN.

- Only trunk ports can join an ERPS ring, and the trunk attributes cannot be modified after the port joins the ring.
- The ports in an ERPS ring do not participate in STP calculation regardless of whether the ERPS ring is enabled or not. When you configure an ERPS ring, ensure that loops will not occur when STP calculation is disabled on ports in the ring.
- ERPS does not use the same ports as RERP and REUP.

Configuration Steps

Configuring the R-APS VLAN of an Ethernet Ring

- (Mandatory) Perform this configuration in global configuration mode.
- Configure the same R-APS VLAN on all switches in the ERPS ring to transmit ERPS packets.

Configuring ERPS Ring Ports

- (Mandatory) Perform this configuration in R-APS VLAN mode.
- Configure the ports that form the ERPS ring as ERPS ring ports.

Configuring an RPL Owner Port

- (Mandatory) Perform this configuration in R-APS VLAN mode.
- Configure a single device in each ERPS ring as an RPL owner node, which will control the port to be blocked.

Enabling the Specified R-APS Ring

- (Mandatory) Perform this configuration in R-APS VLAN mode.
- Enable the specified R-APS ring in the same R-APS VLAN on each switch.

Enabling ERPS Globally

- (Mandatory) Perform this configuration in global configuration mode.
- Enable ERPS globally on each switch in the ERPS ring.

Verification

- Run the **show erps** command one each node to check the configuration.

Related Commands

Configuring the R-APS VLAN of an Ethernet Ring

Command	**erps raps-vlan** *vlan-id*
Parameter Description	*vlan-id*: R-APS VLAN ID
Command Mode	Global configuration mode

Usage Guide	ERPS takes effect in a ring only after ERPS is enabled globally and for the ring respectively.

Configuring an ERPS Ring

Command	**ring-port west** {*interface-name1* | **virtual-channel** } **east** { *interface-name2* | **virtual-channel**}
Parameter Description	*interface-name1*: Indicates the name of the West port. *interface-name2*: Indicates the name of the East port. **virtual-channel:** Assigns a port to a virtual link.
Command Mode	R-APS VLAN mode
Usage Guide	The R-APS VLAN must be the unused VLAN on a device. VLAN 1 cannot be configured as the R-APS VLAN. In an Ethernet ring, different devices must be configured with the same R-APS VLAN. If you need to transparently transmit ERPS packets on a device not configured with ERPS, ensure that only the two ports on the device connected to the ERPS ring allow packets from the R-APS 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.

Configuring an RPL Owner Port

Command	**rpl-port** { **west** | **east** } **rpl-owner**
Parameter Description	**west**: Specifies the West port as an RPL owner port. **east**: Specifies the East port as an RPL owner port.
Command Mode	R-APS VLAN mode
Usage Guide	Each ring can be configured with only one RPL and only one RPL owner node.

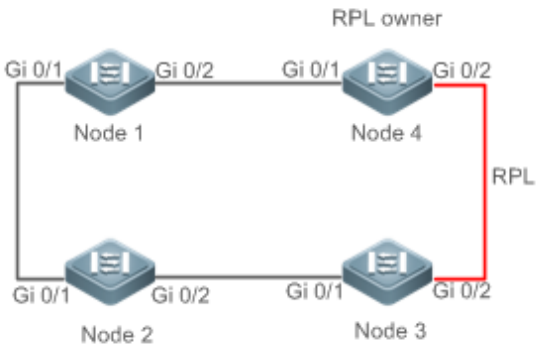
Enabling the Specified R-APS Ring

Command	**state enable**
Parameter Description	N/A
Command Mode	R-APS VLAN mode
Usage Guide	ERPS takes effect in a ring only after ERPS is enabled globally and for the ring respectively.

Enabling ERPS Globally

Command	**erps enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	ERPS takes effect in a ring only after ERPS is enabled globally and for the ring respectively.

Configuration Example

Scenario	
Configuration Steps	● Configure the R-APS VLAN in privileged mode. ● Configure the link mode of ports in the Ethernet ring. ● Enter R-APS VLAN mode and configure the ports to be added to the Ethernet ring and participate in ERPS calculation. ● Specify the RPL owner port. ● Enable ERPS in the specified ring. ● Enable ERPS globally.

Node 1	# Enter privileged mode.
	`Hostname# configure terminal`
	# Configure the R-APS VLAN.
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# exit`
	# Configure the link mode of ports in the Ethernet ring.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/1)# exit`
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/2)# exit`
	# Enter ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 4093`
	# Configure the ports to be added to the Ethernet ring and participate in ERPS calculation.
	`Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2`
	# Enable ERPS in the specified ring.

	Hostname(config-erps 4093)# state enable # Enable ERPS globally. Hostname(config-erps 4093)# exit Hostname(config)# erps enable
Node 2	The configuration on Node 2 is the same as that on Node 1.
Node 3	The configuration on Node 3 is the same as that on Node 1.
Node 4	# Enter privileged mode. Hostname# configure terminal # Configure the R-APS VLAN. Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# exit # Configure the link mode of ports in the Ethernet ring. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/2)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 4093 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 # Specify the RPL owner port. Hostname(config-erps 4093)# rpl-port east rpl-owner # Enable ERPS in the specified ring. Hostname(config-erps 4093)# state enable Hostname(config-erps 4093)# exit # Enable ERPS globally. Hostname(config)# erps enable
Verification	Run the **show erps** command one each node to check the configuration. The configuration on Node 1 and Node 4 is used as an example.

Node 1

```
Hostname# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by                : Not Oam
------------------------------------------
R-APS VLAN                       : 4093
Ring Status                      : Enabled
West Port                        : Gi 0/1 (Forwardin)
East Port                        : Gi 0/2 (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             :
```

Node 4

```
Hostname# show erps
ERPS Information
Global Status                    : Enabled
Link monitored by                : Not Oam
------------------------------------------
R-APS VLAN                       : 4093
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 : 2 minutes Current Ring State : Idle Associate R-APS VLAN :

Common Errors

- The R-APS ring has been enabled but ERPS is not enabled globally, so ERPS still does not take effect.
- Multiple RPL owner nodes are configured in one ring.
- Different R-APS VLANs are configured for the nodes in one ring.

9.4.2 Tangent-Ring Configuration

Configuration Effect

- Configure a tangent ring that consists of two ERPS rings sharing one device to realize data link redundancy.
- Quickly switch services from a failed link in one ERPS ring to a normal link.

Notes

- The tangent-ring configuration is basically the same as the single-ring configuration. You only need to associate the two ERPS rings on the tangent node.
- Only one RPL owner node and only one RPL can be configured in each ERPS ring.
- All nodes in one ERPS ring must belong to the same R-APS VLAN.
- Only trunk ports can join an ERPS ring, and the trunk attributes cannot be modified after the port joins the ring.
- The ports in an ERPS ring do not participate in STP calculation regardless of whether the ERPS ring is enabled or not. When you configure an ERPS ring, ensure that loops will not occur when STP calculation is disabled on ports in the ring.
- ERPS does not use the same ports as RERP and REUP.

Configuration Steps

- The tangent-ring configuration is basically the same as the single-ring configuration. You only need to associate the two ERPS rings on the tangent node.

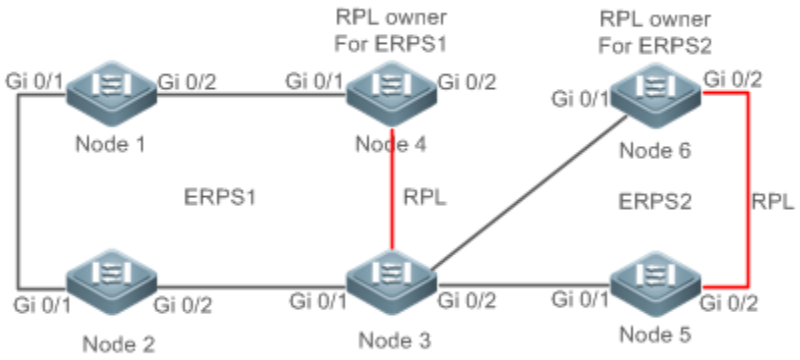
Verification

- Run the **show erps** command one each node to check the configuration.

Related Commands

- See the commands in section 9.4.1 "Single-Ring Configuration (Basic Function)."

Configuration Example

Scenario	
Configuration Steps	● Configure the R-APS VLAN in privileged mode. ● Configure the link mode of ports in the Ethernet ring. ● Enter R-APS VLAN mode and configure the ports to be added to the Ethernet ring and participate in ERPS calculation. ● Specify the RPL owner port. ● Enable ERPS in the specified ring. ● Enable ERPS globally.

Node 1	# Enter privileged mode.
	`Hostname# configure terminal`
	# Configure R-APS VLAN 4093.
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# exit`
	# Configure the link mode of ports in the Ethernet ring.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/1)# exit`
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/2)# exit`
	# Enter ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 4093`
	# Configure the ports to be added to the Ethernet ring and participate in ERPS calculation.
	`Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2`

	# Enable ERPS in the specified ring.
	`Hostname(config-erps 4093)# state enable`
	`Hostname(config-erps 4093)# exit`
	# Enable ERPS globally.
	`Hostname(config)# erps enable`

Node 2	The configuration on Node 2 is the same as that on Node 1.

Node 3	`Hostname# configure terminal`
	# Configure R-APS VLAN 4093.
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# exit`
	# Configure the link mode of ports in the Ethernet ring.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/1)# exit`
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/2)# exit`
	# Enter ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2`
	`Hostname(config-erps 4093)# state enable`
	`Hostname(config-erps 4093)# exit`
	# Configure R-APS VLAN 100.
	`Hostname(config)# erps raps-vlan 100`
	`Hostname(config-erps 100)# exit`
	`Hostname(config)# interface gigabitEthernet 0/3`
	`Hostname(config-if-gigabitEthernet 0/3)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/3)# exit`
	`Hostname(config)# interface gigabitEthernet 0/4`
	`Hostname(config-if-gigabitEthernet 0/4)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/4)# exit`
	# Enter ERPS configuration mode.

	Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# ring-port west gigabitEthernet 0/3 east gigabitEthernet 0/4 Hostname(config-erps 100)# state enable Hostname(config-erps 4093)# exit Hostname(config)# erps enable
Node 4	Hostname# configure terminal # Configure R-APS VLAN 4093. Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# exit # Configure the link mode of ports in the Ethernet ring. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/2)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 # Specify the RPL owner port. Hostname(config-erps 4093)# rpl-port east rpl-owner Hostname(config-erps 4093)# state enable Hostname(config-erps 4093)# exit Hostname(config)# erps enable
Node 5	Hostname# configure terminal # Configure R-APS VLAN 100. Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# exit # Configure the link mode of ports in the Ethernet ring. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk

	Hostname(config-if-gigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/2)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 Hostname(config-erps 100)# state enable Hostname(config-erps 100)# exit Hostname(config)# erps enable
Node 6	Hostname# configure terminal # Configure R-APS VLAN 100. Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# exit # Configure the link mode of ports in the Ethernet ring. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/2)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 # Specify the RPL owner port. Hostname(config-erps 100)# rpl-port east rpl-owner Hostname(config-erps 100)# state enable Hostname(config)# erps enable
Verification	Run the **show erps** command one each node to check the configuration. The configuration on Node 3 is used as an example.
	Hostname# show erps

```
ERPS Information
Global Status                    : Enabled
Link monitored by                : Not Oam
------------------------------------------
R-APS VLAN                       : 100
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                       : 4093
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             :
```

Common Errors

- The R-APS ring has been enabled but ERPS is not enabled globally, so ERPS still does not take effect.

- Multiple RPL owner nodes are configured in one ring.
- Different R-APS VLANs are configured for the nodes in one ring.

9.4.3 Intersecting-Ring Configuration

Configuration Effect

- Configure multiple ERPS rings to share links, thus realizing data link redundancy.
- Quickly switch services from a failed link in one ERPS ring to a normal link.

Notes

- Only one RPL owner node and only one RPL can be configured in each ERPS ring.
- All nodes in one ERPS ring must belong to the same R-APS VLAN.
- All nodes in the Ethernet ring must be associated with their respective subrings.
- Only trunk ports can join an ERPS ring, and the trunk attributes cannot be modified after the port joins the ring.
- The ports in an ERPS ring do not participate in STP calculation regardless of whether the ERPS ring is enabled or not. When you configure an ERPS ring, ensure that loops will not occur when STP calculation is disabled on ports in the ring.
- ERPS does not use the same ports as RERP and REUP.

Configuration Steps

Perform the following configuration after you complete the single-ring configuration described above:

↘ **Enabling Subring Topology Change Notification**

- (Optional) Perform this configuration in R-APS VLAN mode.
- Enable subring topology change notification on intersecting nodes.
- If 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.

↘ **Associating Ethernet Subrings**

- (Optional) Perform this configuration in R-APS VLAN mode.
- Associate nodes in the main ring with Ethernet subrings.
- After nodes are associated with Ethernet subrings, ERPS packets of the subrings can be transmitted to other Ethernet rings.

Verification

- Run the **show erps** command one each node to check the configuration.

Related Commands

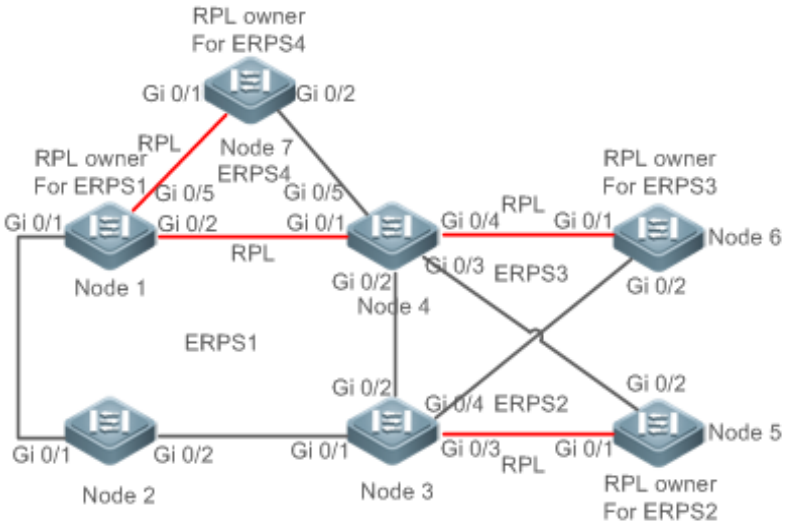
Enabling Subring Topology Change Notification

Command	**sub-ring tc-propagation enable**
Parameter Description	N/A
Command Mode	R-APS VLAN mode
Usage Guide	Run this command only on intersecting nodes.

Associating Ethernet Subrings

Command	**associate sub-ring raps-vlan** *vlan-list*
Parameter Description	*vlan-list*: Indicates the R-APS VLANs of subrings.
Command Mode	R-APS VLAN mode
Usage Guide	Run this command on all nodes in the Ethernet ring to allow its subrings to transmit ERPS packets to the Ethernet ring. After nodes are associated with subrings, ERPS packets of the subrings can be transmitted to other Ethernet rings. You can also use the command provided by the VLAN module to configure VLAN and its member ports to allow ERPS packets of subrings to be transmitted to other Ethernet rings while avoiding information leakage to user networks.

Configuration Example

Scenario	
Configuration	● Configure the R-APS VLAN in privileged mode.

Steps	● Configure the link mode of ports in the Ethernet ring. ● Enter R-APS VLAN mode and configure the ports to be added to the Ethernet ring and participate in ERPS calculation. ● Specify the RPL owner port. ● Enable ERPS in the specified ring. ● Associate nodes in the Ethernet ring with subrings. ● Enable subring topology change notification on intersecting nodes. ● Enable ERPS globally.

Node 1	# Enter privileged mode.
	`Hostname# configure terminal`
	# Configure R-APS VLAN 4093.
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# exit`
	# Configure the link mode of ports in the Ethernet ring.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/1)# exit`
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/2)# exit`
	# Enter ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 4093`
	# Configure the ports to be added to the Ethernet ring and participate in ERPS calculation.
	`Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2`
	# Specify the port and RPL owner node for the RPL.
	`Hostname(config-erps 4093)# rpl-port east rpl-owner`
	# Enable ERPS in the specified ring.
	`Hostname(config-erps 4093)# state enable`
	# Enable ERPS globally.
	`Hostname(config-erps 4093)# exit`
	`Hostname(config)# erps enable`
	# Configure the R-APS VLAN of the subring ERPS 4.
	`Hostname(config)# erps raps-vlan 300`

	Hostname(config-erps 300)# exit # Configure the link mode of ports in ERPS 4. Hostname(config)# interface gigabitEthernet 0/5 Hostname(config-if-gigabitEthernet 0/5)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/5)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 300 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 300)# ring-port west gigabitEthernet 0/5 east virtual-channel # Enable ERPS in ERPS 4. Hostname(config-erps 300)# state enable # Associate ERPS 1 with ERPS 2, ERPS 3, and ERPS 4. Hostname(config-erps 300)# exit Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# associate sub-ring raps-vlan 100,200,300
Node 2	# Enter privileged mode. Hostname# configure terminal # Configure R-APS VLAN 4093. Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# exit # Configure the link mode of ports in the Ethernet ring. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/2)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 4093 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 # Enable ERPS in the specified ring.

	Hostname(config-erps 4093)# state enable # Enable ERPS globally. Hostname(config-erps 4093)# exit Hostname(config)# erps enable # Associate ERPS 1 with ERPS 2, ERPS 3, and ERPS 4. Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# associate sub-ring raps-vlan 100,200,300
Node 3	# Perform the following configuration on Node 3 based on the configuration on Node 2: # Enter privileged mode. Hostname# configure terminal # Configure the R-APS VLAN of the subring ERPS 2. Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# exit # Configure the link mode of ports in ERPS 2. Hostname(config)# interface gigabitEthernet 0/3 Hostname(config-if-gigabitEthernet 0/3)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/3)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 100 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 100)# ring-port west virtual-channel east gigabitEthernet 0/3 # Enable ERPS in ERPS 2. Hostname(config-erps 100)# state enable # Configure the R-APS VLAN of the subring ERPS 3. Hostname(config)# erps raps-vlan 200 Hostname(config-erps 200)# exit # Configure the link mode of ports in ERPS 3. Hostname(config)# interface gigabitEthernet 0/4 Hostname(config-if-gigabitEthernet 0/4)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/4)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 200

	# Configure the ports to be added to the Ethernet ring and participate in ERPS calculation.
	`Hostname(config-erps 200)# ring-port west virtual-channel east gigabitEthernet 0/4`
	# Enable ERPS in ERPS 2.
	`Hostname(config-erps 200)# state enable`
	# Associate the Ethernet subrings ERPS 2, ERPS 3, and ERPS 4.
	`Hostname(config-erps 200)# exit`
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# associate sub-ring raps-vlan 100,200,300`

Node 4	# Perform the following configuration on Node 4 based on the configuration on Node 2.
	# Enter privileged mode.
	`Hostname# configure terminal`
	# Configure the R-APS VLAN of the subring ERPS 2.
	`Hostname(config)# erps raps-vlan 100`
	`Hostname(config-erps 100)# exit`
	# Configure the link mode of ports in ERPS 2.
	`Hostname(config)# interface gigabitEthernet 0/3`
	`Hostname(config-if-gigabitEthernet 0/3)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/3)# exit`
	# Enter ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 100`
	# Configure the ports to be added to the Ethernet ring and participate in ERPS calculation.
	`Hostname(config-erps 100)# ring-port west virtual-channel east gigabitEthernet 0/3`
	# Enable ERPS in ERPS 2.
	`Hostname(config-erps 100)# state enable`
	# Configure the R-APS VLAN of the subring ERPS 3.
	`Hostname(config)# erps raps-vlan 200`
	`Hostname(config-erps 200)# exit`
	# Configure the link mode of ports in ERPS 3.
	`Hostname(config)# interface gigabitEthernet 0/4`
	`Hostname(config-if-gigabitEthernet 0/4)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/4)# exit`
	# Enter ERPS configuration mode.

	Hostname(config)# erps raps-vlan 200 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 200)# ring-port west virtual-channel east gigabitEthernet 0/4 # Enable ERPS in ERPS 3. Hostname(config-erps 200)# state enable # Configure the R-APS VLAN of the subring ERPS 4. Hostname(config-erps 200)# exit Hostname(config)# erps raps-vlan 300 Hostname(config-erps 300)# exit # Configure the link mode of ports in ERPS 4. Hostname(config)# interface gigabitEthernet 0/5 Hostname(config-if-gigabitEthernet 0/5)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/5)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 300 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 300)# ring-port west virtual-channel east gigabitEthernet 0/5 # Enable ERPS in ERPS 4. Hostname(config-erps 300)# state enable # Associate the Ethernet subrings ERPS 2, ERPS 3, and ERPS 4. Hostname(config-erps 300)# exit Hostname(config)# erps raps-vlan 4093 Hostname(config-erps4093)# associate sub-ring raps-vlan 100,200,300
Node 5	# Enter privileged mode. Hostname# configure terminal # Configure the R-APS VLAN. Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# end # Configure the link mode of ports in the Ethernet ring. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk

	Hostname(config-if-gigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk Hostname(config-if-gigabitEthernet 0/2)# exit # Enter ERPS configuration mode. Hostname(config)# erps raps-vlan 100 # Configure the ports to be added to the Ethernet ring and participate in ERPS calculation. Hostname(config-erps 100)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 # Specify the port and RPL owner node for the RPL. Hostname(config-erps 100)# rpl-port east rpl-owner # Enable ERPS in the specified ring. Hostname(config-erps 100)# state enable # Enable ERPS globally. Hostname(config-erps 100)# exit Hostname(config)# erps enable
Node 6	# The configuration on Node 6 is basically the same as that on Node 5, except that you need to change the R-APS VLAN to VLAN 200.
Node 7	# The configuration on Node 7 is basically the same as that on Node 5, except that you need to change the R-APS VLAN to VLAN 300.
Verification	Run the **show erps** command one each node to check the configuration. The configuration on Node 3 is used as an example.
	Hostname# show erps ERPS Information Global Status : Enabled Link monitored by : Not Oam ---------- R-APS VLAN : 100 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                      : 200
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                      : 4093
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            : 100,200,300
```

Common Errors

- The R-APS ring has been enabled but ERPS is not enabled globally, so ERPS still 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 man ring are not associated with Ethernet subrings.

9.4.4 Load Balancing Configuration

Configuration Effect

- Control the direction of data flows in an ERPS ring to realize load balancing.
- When a link in the ring network enabled with load balancing fails, the traffic can be quickly switched to a normal link.

Notes

- Before you configure load balancing, configure the VLAN-instance relationship 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 will cause loops.
- Only trunk ports can join an ERPS ring, and the trunk attributes cannot be modified after the port joins the ring.
- The ports in an ERPS ring do not participate in STP calculation regardless of whether the ERPS ring is enabled or not. When you configure an ERPS ring, ensure that loops will not occur when STP calculation is disabled on ports in the ring.
- ERPS does not use the same ports as RERP and REUP.

Configuration Steps

Perform the following configuration after you complete the single-ring configuration described above:

↘ Configuring the Protected VLAN of an Ethernet Ring

- (Optional) Perform this configuration in global configuration mode.
- When you configure load balancing for an Ethernet ring, you must specify the protected VLAN.

Verification

- Run the **show erps** command one each node to check the configuration.

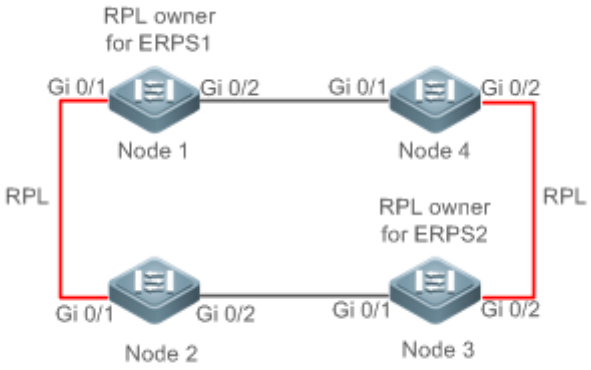
Related Commands

↘ Configuring the Protected VLAN of an Ethernet Ring

Command	**protected-instance** *instance-id-list*
Parameter	*instance-id-list*: Indicates the instance protected by the Ethernet ring.

Description	
Command Mode	R-APS VLAN mode
Usage Guide	The protected instance of the Ethernet ring is the protected VLAN.

Configuration Example

Scenario	
Configuration Steps	● Configure the R-APS VLAN in privileged mode. ● Configure the link mode of ports in the Ethernet ring. ● Configure the protected VLAN of the Ethernet ring. ● Enter R-APS VLAN mode and configure the ports to be added to the Ethernet ring and participate in ERPS calculation. ● Specify the RPL owner port. ● Enable ERPS in the specified ring. ● Enable ERPS globally.

Node 1	# Enter privileged mode.
	`Hostname# configure terminal`
	# Configure the Ethernet subring ERPS 1 as follows:
	# Configure the link mode of ports in ERPS 1.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/1)# exit`
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/2)# exit`
	# Configure the protected VLAN, RPL owner port, and RPL of ERPS 1.
	`Hostname(config)# spanning-tree mst configuration`

	Hostname(config-mst)# instance 1 vlan 1-2000 Hostname(config-mst)# exit Hostname(config)# erps raps-vlan 100 Hostname(config-erps 100)# protected-instance 1 Hostname(config-erps 100)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 Hostname(config-erps 100)# rpl-port west rpl-owner # Configure the Ethernet subring ERPS 2 as follows: # Configure the ports to be added to ERPS 2 and participate in ERPS calculation. Hostname(config)# spanning-tree mst configuration Hostname(config-mst)# instance 2 vlan 2001-4094 Hostname(config-mst)# exit Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# protected-instance 2 Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/2 # Enable ERPS in ERPS 2 and globallyrespectively. Hostname(config-erps 4093)# state enable Hostname(config-erps 4093)# exit Hostname(config)# erps enable
Node 2	# The configuration on Node 2 is the same as that on Node 1, except that RPL configuration is not required on Node 2.
Node 3	# The configuration on Node 3 is the same as that on Node 1, except that RPL configuration is not required on Node 3. # Configure the RPL of ERPS 2 on Node 3. The RPL of ERPS 1 does not need to be configured on Node 3. Hostname(config)# erps raps-vlan 4093 Hostname(config-erps 4093)# rpl-port east rpl-owner
Node 4	The configuration on Node 4 is the same as that on Node 2.
Verification	Run the **show erps** command one each node to check the configuration. The configuration on Node 1 is used as an example.
Node 1	Hostname# show erps ERPS Information Global Status : Enabled Link monitored by : Not Oam

```
------------------------------------------
R-APS VLAN                    : 200
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                    : 4093
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          :
```

Common Errors

- The R-APS ring has been enabled but ERPS is not enabled globally, so ERPS still 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.

9.4.5 ERPS Configuration Modification

Configuration Effect

- Switch configuration smoothly when the ERPS ring topology is changed.

Notes

- When you modify the ERPS configuration on a device, to avoid loops, first run the **shutdown** command to shut down an ERPS port in the ring. When the configuration is completed, run the **no shutdown** command to restart the port.
- All nodes in one ERPS ring must belong to the same R-APS VLAN.
- If you only need to modify the ERPS timers, skip this section.

Configuration Steps

Run the **shutdown** command to shut down an ERPS port and disable ERPS. Then modify the ERPS configuration according to section 9.4.1 "Single-Ring Configuration (Basic Function)" and complete the following settings, which are optional.

↘ **Configuring the Holdoff Timer, Guard Timer, and WRT Timer**

- Optional.
- Perform this configuration in R-APS VLAN mode based on the actual application requirements.

Verification

- Run the **show erps** command one each node to check the configuration.

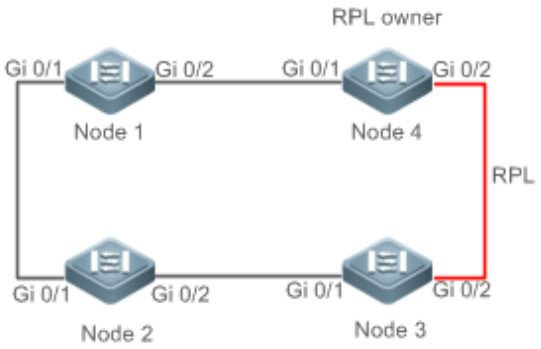
Related Commands

↘ **Configuring the Holdoff Timer, Guard Timer, and WRT Timer**

Command	**timer** { **holdoff-time** *interval1* | **guard-time** *interval2* | **wtr-time** *interval3* }
Parameter Description	*interval1:* Indicates the Holdoff timer interval. The value ranges from 0 to 100, in the unit of 100 milliseconds. The default value is 0. *interval2:* Indicates the Guard timer interval. The value ranges from 1 to 200, in the unit of 10 milliseconds. The default value is 50. *interval3:* Indicates the WTR timer interval. The value ranges from 1 to 12, in the unit of minutes. The default value is 2.
Command Mode	R-APS VLAN mode
Usage Guide	● Holdoff 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: Is used to prevent a device from receiving expired R-APS messages. When the device detects that a link failure is cleared, it sends link recovery packets and starts the Guard timer. During

	the period before timer expiration, all packets except flush packets indicating a subring topology change will be discarded. ● WTR timer: Is effective only for RPL owner devices to avoid ring status misjudgment. When an RPL owner device detects that a failure is cleared, it does 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 timer expiration, the RPL owner device cancels the timer and does not perform topology switching.

Configuration Example

Scenario	
Configuration Steps	● ERPS configuration exists in the ring. The ERPS ports need to be switched because of a physical topology change. ● Run the **shutdown** command to shut down a link in the ring and configure the link mode of ports after switching. ● Disable ERPS in the ring in R-APS VLAN mode. ● Reconfigure the ports that will participate in ERPS calculation. ● Enable ERPS in the ring. ● Modify the ERPS timers.

Node 1	# Enter privileged mode.
	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	# Shutdown a link in the ring in interface configuration mode to avoid loops.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)# shutdown`
	`Hostname(config-if-gigabitEthernet 0/1)# exit`
	# Configure the link mode of ports in the Ethernet ring.
	`Hostname(config)# interface gigabitEthernet 0/3`
	`Hostname(config-if-gigabitEthernet 0/3)# switchport mode trunk`
	`Hostname(config-if-gigabitEthernet 0/3)# exit`

	# Enter ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 4093`
	# Disable ERPS.
	`Hostname(config-erps 4093)# no state enable`
	# Delete the previous ring configuration.
	`Hostname(config-erps 4093)# no ring-port`
	# Reconfigure the ports that will participate in ERPS calculation. Change Gig 0/2 to Gig 0/3.
	`Hostname(config-erps 4093)# ring-port west gigabitEthernet 0/1 east gigabitEthernet 0/3`
	# Enable ERPS.
	`Hostname(config-erps 4093)# state enable`

Node 4	# Enter privileged mode.
	`Hostname# configure terminal`
	# Modify timers in ERPS configuration mode.
	`Hostname(config)# erps raps-vlan 4093`
	`Hostname(config-erps 4093)# timer wtr-time 1`

	Wait for 1 minute. When the ERPS ring is restored to Idle, run the **show erps** command on Node 1 and Node 4 to check the configuration.

Node 1	`Hostname# show erps`
	`ERPS Information`
	`Global Status : Enabled`
	`Link monitored by : Not Oam`
	`----------`
	`R-APS VLAN : 4093`
	`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 :
Node 4	Hostname# show erps ERPS Information Global Status : Enabled Link monitored by : Not Oam ---------- R-APS VLAN : 4093 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 :

Common Errors

- When the configuration is completed, the R-APS ring is not enabled again or the shutdown ports are not restarted by using the **no shutdown** command.

9.5 Monitoring

Displaying

Description	Command
Displays the ERPS configuration and status of devices.	**show erps** [**global** | **raps_vlan** *vlan-id* [*sub_ring*]]

IP Address & Application Configuration

1. Configuring IP Address and Service
2. Configuring ARP
3. Configuring IPv6
4. Configuring DHCP
5. Configuring DNS
6. Configuring TFTP Client
7. Configuring Network Communication Detection Tools
8. Configuring TCP
9. Configuring IPv4/IPv6 REF

1 Configuring IP Addresses and Services

1.1 Overview

Internet Protocol (IP) sends packets to the destination from the source by using logical (or virtual) addresses, namely IP addresses. At the network layer, routers forward packets based on IP addresses.

Protocols and Standards

- RFC 1918: Address Allocation for Private Internets
- RFC 1166: Internet Numbers

1.2 Applications

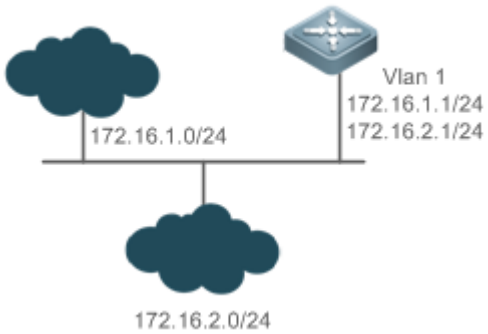
Application	Description
Configuring an IP Address for Communication	Two networks communicate through one switch interface.

1.2.1 Configuring an IP Address for Communication

Scenario

A switch is connected to a Local Area Network (LAN), which is divided into two network segments , namely, 172.16.1.0/24 and 172.16.2.0/24. Computers in the two network segments can communicate with the Internet through switches and computers between the two network segments can communicate with each other.

Figure 1-1 Configuring IP Addresses



Deployment

- Configure two IP addresses on VLAN1. One is a primary IP address and the other is a secondary IP address.
- On hosts in the network segment 172.16.1.0/24, set the gateway to 172.16.1.1; on hosts in the network segment 172.16.2.0/24, set the gateway to 172.16.2.1.

1.3 Features

Basic Concepts

IP Address

An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal. When expressed in decimal, 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 a full stop ".". For example, "192.168.1.1" is an IP address expressed in decimal.

IP addresses are used for interconnection at the IP layer. A 32-bit IP address consists of two parts, namely, the network bits and the host bits. 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 0.7 bits indicate a network ID, and 24 bits indicate a local address. There are 128 class A networks in total.

Figure 1-2

		8	16 32	24
Class A IP address		Network ID	Host ID	

For a class B address, the first two most significant bits are 10.14 bits indicate a network ID, and 16 bits indicate a local address. There are 16,348 class B networks in total.

Figure 1-3

			8	16 32	24
Class B IP address			Network ID	Host ID	

For a class C address, the first three most significant bits are 110.21 bits indicate a network ID, and 8 bits indicate a local address. There are 2,097,152 class C networks in total.

Figure 1-4

				8	16	24	32
Class C IP address				Network ID		Host ID	

For a class D address, the first four most significant bits are 1110 and other bits indicate a multicast address.

Figure 1-5

					8	16	24	32
Class D IP address					Multicast address			

The addresses with the first four most significant bits 1111 cannot be assigned. These addresses are called class E addresses and are reserved.

When IP addresses are planned during network construction, IP addresses must be assigned based on the property of the network to be built. If the network needs to be connected to the Internet, users should apply for IP addresses to

the corresponding agency. In China, you can apply to China Internet Network Information Center (CNNIC) for IP addresses. Internet Corporation for Assigned Names and Numbers (ICANN) is the final organization responsible for IP address assignment. If the network to be built is an internal private network, users do not need to apply for IP addresses. However, IP addresses cannot be assigned at random. It is recommended to assign dedicated private network addresses.

The following table lists 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 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 address
Class E network	240.0.0.0 - 255.255.255.254	Reserved
	255.255.255.255	Broadcast address

Three address ranges are dedicated to private networks. These addresses are not used in the Internet. If the networks to which these addresses are assigned need to be connected to the Internet, these IP addresses need to be converted into valid Internet addresses. The following table lists private address ranges. Private network addresses are defined in RFC 1918.

Class	Address Range	Status
Class A network	10.0.0.0 - 10.255.255.255	1 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/UDP ports, and other codes, refer to RFC 1166.

Subnet Mask

A subnet mask is also a 32-bit value. The bits that identify the IP address are the network address. In a subnet mask, the IP address bits corresponding to the bits whose values are 1s are the network address, and the IP address bits corresponding to the bits whose values are 0s are the host address. For example, for class A networks, the subnet mask is 255.0.0.0. By using network masks, you can divide a network into several subnets. Subnetting means to use some bits of the host address as the network address, thus decreasing the host capacity, and increasing the number of networks. In this case, network masks are called subnet masks.

Broadcast Packet

Broadcast packets refer to the packets destined for all hosts on a physical network. The products support two types of broadcast packets: (1) directed broadcast, which indicates that all hosts on the specified network are packet receivers and the host bits of a destination address are all 1s; (2) limited broadcast, which indicates that all hosts on all networks are packet receivers and the 32 bits of a destination address are all 1s.

ICMP Packet

Internet Control Message Protocol (ICMP) is a sub-protocol in the TCP/IP suite for transmitting control messages between IP hosts and network devices. It is mainly used to notify corresponding devices when the network performance becomes abnormal.

TTL

Time To Live (TTL) refers to the number of network segments where packets are allowed to pass before the packets are discarded. The TTL is a value in an IP packet. It informs the network whether packets should be discarded as the packets stay on the network for a long time.

Features

Feature	Description
IP Address	The IP protocol can run on an interface only after the interface is configured with an IP address.
Broadcast Packet Processing	Broadcast addresses are configured and broadcast packets are forwarded and processed.
Sending ICMP Packets	ICMP packets are sent and received.
Limiting Transmission Rate of ICMP Error Packets	This function prevents Denial of Service (DoS) attacks.
IP MTU	Maximum Transmission Unit (MTU) of IP packets on an interface is configured.
IP TTL	The TTL of unicast packets and broadcast packets is configured.
IP Source Route	Source routes are checked.
IP Address Pool	An IP address is assigned to the peer end during PPP negotiation.

1.3.1 IP Address

IP addresses are obtained on an interface in the following ways:

1. Manually configuring IP addresses
2. Obtaining IP addresses through DHCP
3. Obtaining IP addresses through PPP negotiation

These approaches are mutually exclusive. If you configure a new approach to obtain an IP address, the old IP address will be overwritten.

For details on how to obtain IP addresses through DHCP, see the “DHCP” chapter. The following describes the other three approaches for obtaining IP addresses.

Configuring the IP Address for an Interface

A device can receive and send IP packets only after the device is configured with an IP address. Only the interface configured with an IP address can run the IP protocol.

Configuring Multiple IP Addresses for an Interface

The products support multiple IP address configuration on one interface, of which one is a primary IP address and the others are secondary IP addresses or slave 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, a LAN now needs one class C network to allocate 254 addresses. However, when the number of hosts exceeds 254, 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 L2 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, you can connect the isolated subnets by creating a subnet of the isolated network and configuring a secondary address. One subnet cannot be configured on two or more interfaces of a device.

Obtaining an IP Addresses through PPP Negotiation

This command is supported on point-to-point interfaces only.

Through this configuration, a point-to-point interface accepts the IP address assigned by the peer end through PPP negotiation.

Related Configuration

Configuring an Interface with One or More IP Addresses

- By default, an interface is not configured with an IP address.
- The **ip address** command is used to configure an IP address for an interface.
- After an IP address is configured, the IP address can be used for communication when it passes conflict detection.
- The **ip address** *ip-address mask* **secondary** command can be used to configure multiple secondary IP addresses.

1.3.2 Broadcast Packet Processing

Working Principle

Broadcast is divided into two types. One is limited broadcast, and the IP address is 255.255.255.255. Because the broadcast is prohibited by routers, the broadcast is called local network broadcast. The other is directed broadcast. All host bits are 1s, for example, 192.168.1.255/24. The broadcast packets with these IP addresses can be forwarded.

If IP network devices forward limited broadcast packets (destination IP address is 255.255.255.255), the network may be overloaded, which severely affects network performance. This circumstance is called broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. L2 network devices such as bridges and switches forward and spread broadcast storms.

The best way to avoid broadcast storm is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast rather than limited broadcast to spread data.

For details about broadcast storms, see RFC 919 and RFC 922.

Directed broadcast packets refer to the broadcast packets destined for a subnet. For example, packets whose destination address is 172.16.16.255 are called directed broadcast packets. However, the node that generates the packets is not a member of the destination subnet.

After receiving directed broadcast packets, the devices not directly connected to the destination subnet forward the packets. After directed broadcast packets reach the devices directly connected to the subnet, the devices convert directed broadcast packets to limited broadcast packets (destination IP address is 255.255.255.255) and broadcast the packets to all hosts on the destination subnet at the link layer.

Related Configuration

Configuring an IP Broadcast Address

- By default, the IP broadcast address of an interface is 255.255.255.255.
- To define broadcast packets of other addresses, run the **ip broadcast-address** command on the interface.

Forwarding Directed Broadcast Packets

- By default, directed broadcast packets cannot be forwarded.
- On the specified interface, you can run the **ip directed-broadcast** command to enable directed broadcast packets forwarding. In this way, the interface can forward directed broadcast packets to networks that are directly

connected. Broadcast packets can be transmitted within the destination subnet without affecting forwarding of other directed broadcast packets.

- On an interface, you can define an Access Control List (ACL) to transmit certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.3.3 Sending ICMP Packets

Working Principle

ICMP Protocol Unreachable Message

A device receives non-broadcast packets destined for itself, and the packets contain the IP protocol that cannot be processed by the device. The device sends an ICMP protocol unreachable message to the source host. Besides, if the device does not know a route to forward packets, it also sends an ICMP host unreachable message.

ICMP Redirection Message

Sometimes, a route may be less than optimal, which makes a device send packets from the interface that receives packets. If a device sends packets from an interface on which it receives the packets, the device sends an ICMP redirection message to the source, informing the source that the gateway is another device on the same subnet. In this way, the source sends subsequent packets according to the optimal path.

ICMP Mask Response 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 response message.

Error Message for TTL Timeout

When forwarding an IP packet of which TTL expires, a device responds to the source end with an error message indicating exceeded TTL. To prevent attacks after the route is traced, the functionality of sending such error messages can be disabled.

Timestamp Query

RFC 792 requires the system, after receiving an ICMP timestamp request query message, to return its current time. You can disable sending of such reply messages to avoid attacks aimed at time-based protocols. By this means, once received, ICMP timestamp request query messages are discarded.

Related Configuration

Enabling ICMP Protocol Unreachable Message

- By default, the ICMP Protocol unreachable message function is enabled on an interface.
- You can run the [**no**] **ip unreachables** command to disable or enable the function.

Enabling ICMP Redirection Message

- By default, the ICMP redirection message function is enabled on an interface.
- You can run the [**no**] **ip redirects** command to disable or enable the function.

Enabling ICMP Mask Response Message

- By default, the ICMP mask response message function is enabled on an interface.
- You can run the [**no**] **ip mask-reply** command to disable or enable the function.

Enabling Error Message for TTL Timeout

- By default, the error message for TTL timeout function is enabled.
- You can run the [**no**] **ip ttl-expires enable** command to disable or enable the function.

Enabling Timestamp Query

- By default, the timestamp query function is enabled on an interface.
- You can run the [**no**] **ip icmp timestamp** command to disable or enable the function.

1.3.4 Limiting Transmission Rate of ICMP Error Packets

Working Principle

This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm.

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 packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) 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 packets and other ICMP error packets respectively.

Related Configuration

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by DF Bit in the IP Header

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval DF** command can be used to configure the transmission rate.

Configuring the Transmission Rate of Other ICMP Error Packets

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval** command can be used to configure the transmission rate.

1.3.5 IP MTU

Working Principle

If an IP packet exceeds the IP MTU size, the system segments the packet. For all devices in the same physical network segment, the IP MTU of interconnected interfaces must be the same. You can adjust the link MTU of interfaces on the products. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed. 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.

Related Configuration

Setting the IP MTU

- By default, the IP MTU of an interface is 1500.
- The **ip mtu** command can be used to set the IP packet MTU.

1.3.6 IP TTL

Working Principle

An IP packet is transmitted from the source address to the destination address through routers. After a TTL value is set, the TTL value decreases by 1 every time when the IP packet passes a router. When the TTL value drops to zero, the router discards the packet. This prevents infinite transmission of useless packets and waste of bandwidth.

Related Configuration

Setting the IP TTL

- By default, the IP TTL of an interface is 64.
- The **ip ttl** command can be used to set the IP TTL of an interface.

1.3.7 IP Source Route

Working Principle

The products support IP source routes. When a device receives an IP packet, it checks the options such as 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 responds; if the device detects an invalid option, it sends an ICMP parameter error message to the source and then discards the packet.

After the IP source route is enabled, the source route option is added to an IP packet to test the throughput of a specific network or help the packet bypasses the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

Related Configuration

Configuring an IP Source Route

- By default, the IP source route function is enabled.
- The **ip source-route** command can be used to enable or disable the function.

1.4 Configuration

Configuration	Description and Command	
Configuring the IP Addresses of an Interface	⚠ (Mandatory) It is used to configure an IP address and allow the IP protocol to run on an interface.	
	ip address	Manually configures the IP address of an interface.
Configuring Broadcast Forwarding	⚠ (Optional) It is used to set an IP broadcast address and enable directed broadcast forwarding.	
	ip broadcast-address	Configures an IP broadcast address.
	ip directed-broadcast	Enables directed broadcast forwarding.
Configuring ICMP Forwarding	⚠ (Optional) It is used to enable ICMP packet forwarding.	
	ip unreachables	Enables ICMP unreachable messages and host unreachable messages.
	ip redirects	Enables ICMP redirection messages.
	ip mask-reply	Enables ICMP mask response messages.
Configuring the Transmission Rate of	⚠ Optional.	

Configuration	Description and Command	
ICMP Error Packets	**ip icmp error-interval DF**	Configures the transmission rate of ICMP destination unreachable packets triggered by the DF bit in the IP header.
	ip icmp error-interval	Configures the transmission rate of ICMP error packets and ICMP redirection packets.
Setting the IP MTU	(Optional) It is used to configure the IP MTU on an interface.	
	ip mtu	Sets the MTU value.
Setting the IP TTL	(Optional) It is used to configure the TTL of unicast packets and broadcast packets.	
	ip ttl	Sets the TTL value.
Configuring an IP Source Route	(Optional) It is used to check the source routes.	
	ip source-route	Enables the IP source route function.

1.4.1 Configuring the IP Addresses of an Interface

Configuration Effect

Configure the IP address of an interface for communication.

Notes

- N/A

Configuration Steps

Configuring the IP Address of an Interface

- Mandatory
- Perform the configuration in L3 interface configuration mode.

Obtaining the IP Address of an Interface through PPP Negotiation

- Optional
- If a point-to-point interface is not configured with an IP address, obtain an IP address through PPP negotiation.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Manually Configuring the IP Address of an Interface

Command	**ip address** *ip-address network-mask* [**secondary**]
Parameter Description	*ip-address*: 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal and groups are separated by a full stop (.). *network-mask*: 32-bit network mask. Value 1 indicates the mask bit and 0 indicates the host bit. Every 8 bits form one group. The network mask is expressed in decimal and groups are separated

	by a full stop (.). **secondary**: Secondary IP address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring an IP Address for an Interface

Configuration Steps	Configure IP address 192.168.23.110 255.255.255.0 on interface GigabitEthernet 0/0.
	Hostname#configure terminal Hostname(config)#interface gigabitEthernet 0/0 Hostname(config-if-GigabitEthernet 0/0)# no switchport Hostname(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Hostname# show ip interface gigabitEthernet 0/0 GigabitEthernet 0/0 IP interface state is: UP IP interface type is: BROADCAST IP interface MTU is: 1500 IP address is: 192.168.23.110/24 (primary)

1.4.2 Configuring Broadcast Forwarding

Configuration Effect

Set the broadcast address of an interface to 0.0.0.0 and enable directed broadcast forwarding.

Notes

N/A

Configuration Steps

Configuring an IP Broadcast Address

- (Optional) Some old hosts may identify broadcast address 0.0.0.0 only. In this case, set the broadcast address of the target interface to 0.0.0.0.
- Perform the configuration in L3 interface configuration mode.

Enabling Directed Broadcast Forwarding

- (Optional) If you want to enable a host to send broadcast packets to all hosts in a domain that it is not in, enable directed broadcast forwarding.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show running-config interface** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Broadcast Address

Command	**ip broadcast-address** *ip-address*
Parameter Description	*ip-address*: Broadcast address of an IP network.
Command Mode	Interface configuration mode
Usage Guide	Generally, the destination address of IP broadcast packets is all 1s, which is expressed as 255.255.255.255. The system software can generate broadcast packets of other IP addresses through definition and receive self-defined broadcast packets and the broadcast packets with address 255.255.255.255.

Allowing Forwarding of Directed Broadcast Packets

Command	**ip directed-broadcast** [*access-list-number*]
Parameter Description	*access-list-number*: Access list number, ranging from 1 to 199 and from 1300 to 2699. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.
Command Mode	Interface configuration mode
Usage Guide	If the **no ip directed-broadcast** command is run on an interface, the system software will discard directed broadcast packets received from the network that is directly connected.

Configuration Example

Configuration Steps	On interface gigabitEthernet 0/1, set the destination address of IP broadcast packets to 0.0.0.0 and enable directed broadcast forwarding.
	`Hostname#configure terminal`
	`Hostname(config)#interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# no switchport`
	`Hostname(config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0`
	`Hostname(config-if-GigabitEthernet 0/1)#ip directed-broadcast`

Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	`Hostname#show running-config interface gigabitEthernet 0/1`
	`ip directed-broadcast`
	`ip broadcast-address 0.0.0.0`

1.4.3 Configuring ICMP Forwarding

Configuration Effect

Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on an interface.

Notes

N/A

Configuration Steps

Enabling ICMP Unreachable Messages

- By default, ICMP unreachable messages are enabled.
- (Optional) The **no ip unreachables** command can be used to disable ICMP unreachable messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Redirection Messages

- By default, ICMP redirection messages are enabled.
- (Optional) The **no ip redirects** command can be used to disable ICMP redirection messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Mask Response Messages

- By default, ICMP mask response messages are enabled.
- (Optional) The **no ip mask-reply** command can be used to disable ICMP mask response messages.
- Perform the configuration in L3 interface configuration mode.

Enabling Error Messages for TTL Timeout

- By default, error messages for TTL timeout are enabled.
- (Optional) The **no ip ttl-expires enable** command can be used to disable error messages for TTL timeout.
- Perform the configuration in global configuration mode.

Enabling Timestamp Query

- By default, timestamp query is enabled.
- (Optional) The **no ip icmp timestamp** command can be used to disable timestamp query.
- Perform the configuration in global configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Enabling ICMP Unreachable Messages

Command	**ip unreachables**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Redirection Messages

Command	**ip redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Mask Response Messages

Command	**ip mask-reply**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling Error Messages for TTL Timeout

Command	**no ip ttl-expires enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Timestamp Query

Command	**no ip icmp timestamp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on interface gigabitEthernet 0/1.

	`Hostname#configure terminal`
	`Hostname(config)#interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# no switchport`
	`Hostname(config-if-GigabitEthernet 0/1)# ip unreachables`
	`Hostname(config-if-GigabitEthernet 0/1)# ip redirects`
	`Hostname(config-if-GigabitEthernet 0/1)# ip mask-reply`

Verification	Run the **show ip interface** command to check whether the configuration takes effect.

	`Hostname#show ip interface gigabitEthernet 0/1`
	`GigabitEthernet 0/1`
	`  ICMP mask reply is: ON`
	`  Send ICMP redirect is: ON`
	`  Send ICMP unreachabled is: ON`

1.4.4 Configuring the Transmission Rate of ICMP Error Packets

Configuration Effect

Configure the transmission rate of ICMP error packets.

Notes

N/A

Configuration Steps

↘ **Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header**

- Optional
- Perform the configuration in global configuration mode.

Configuring the Transmission Rate of Other ICMP Error Packets

- Optional
- Perform the configuration in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

Command	**ip icmp error-interval DF** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is from 0 to 2,147,483,647 and the default value is 100 milliseconds. When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. If an IP packet needs to be fragmented but the DF bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) 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 packets and other ICMP error packets respectively. It is recommended to set the refresh cycle to integral multiples 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 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10milliseconds.

Configuring the Transmission Rate of Other ICMP Error Packets

Command	**ip icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is 0to 2,147,483,647, and the default value is **100** (ms). When the value is **0**, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is 1to 200 and the default value is **10**.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. It is recommended to set the refresh cycle to integral multiples 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 1 per 5 milliseconds, the refresh

	rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds.

Configuration Example

Configuration Steps	Set the transmission rate of ICMP destination unreachable packets triggered the DF bit in IP header to 100 packets per second and the transmission rate of other ICMP error packets to 10 packets per second.
	`Hostname(config)# ip icmp error-interval DF 1000 100` `Hostname(config)# ip icmp error-interval 1000 10`
Verification	Run the **show running-config** command to check whether the configuration takes effect.

	`Hostname#show running-config | include ip icmp error-interval`
	`ip icmp error-interval 1000 10`
	`ip icmp error-interval DF 1000 100`

1.4.5 Setting the IP MTU

Configuration Effect

Adjust the IP packet MTU.

Notes

N/A

Configuration Steps

- (Optional) When the IP MTU of interconnected interfaces is different on devices in the same physical network segment, set the IP MTU to the same value.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

↘ Setting the IP MTU

Command	**ip mtu***bytes*
Parameter Description	*bytes*: IP packet MTU. The value range is from 68 to 1,500 bytes.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the IP MTU of interface gigabitEthernet 0/1 to 512 bytes.
	Hostname#configure terminal Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# no switchport Hostname(config-if-GigabitEthernet 0/1)#ip mtu 512
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Hostname# show ip interface gigabitEthernet 0/1 IP interface MTU is: 512

1.4.6 Setting the IP TTL

Configuration Effect

Modify the IP TTL value of an interface.

Notes

N/A

Configuration Steps

- Optional
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Setting the IP TTL

Command	**ip ttl** *value*
Parameter Description	*value*: TTL value. The value range is from 0 to 255.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	● Set the TTL of unicast packets to 100.
	`Hostname#configure terminal` `Hostname(config)#ip ttl 100`
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	`Hostname#show running-config` `ip ttl 100`

1.4.7 Configuring an IP Source Route

Configuration Effect

Enable or disable the IP source route function.

Notes

N/A

Configuration Steps

- By default, the IP source route function is enabled.
- (Optional) The **no ip source-route** command can be used to disable the IP source route function.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Source Route

Command	**ip source-route**
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	● Disable the IP source route function.

	Hostname#configure terminal Hostname(config)#no ip source-route
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Hostname#show running-config no ip source-route

1.5 Monitoring

Displaying

Description	Command
Displays the IP address of an interface.	**show ip interface** [*interface-typeinterface-number* | **brief**]
Displays IP packet statistics.	**show ip packet statistics** [**total** | *interface-name*]
Displays statistics on sent and received IP packets in the protocol stack.	**show ip packet queue**

2 Configuring ARP

2.1 Overview

In a local area network (LAN), each IP network device has two addresses: (1) local address. Since the local address is contained in the header of the data link layer (DLL) frame, it is a DLL address. However, it is processed by the MAC sublayer at the DLL and thereby is usually called the MAC address. MAC addresses represent IP network devices on LANs. (2) network address. Network addresses on the Internet represent IP network devices and also indicate the networks where the devices reside.

In a LAN, two IP devices can communicate with each other only after they learn the 48-bit MAC address of each other. The process of obtaining the MAC address based on the IP address is called address resolution. There are two types of address resolution protocols: 1) Address Resolution Protocol (ARP); 2) Proxy ARP. ARP and Proxy ARP are described respectively in RFC 826 and RFC 1027.

ARP is used to bind the MAC address with the IP address. When you enter an IP address, you can learn the corresponding MAC address through ARP. Once the MAC address is obtained, the IP-MAC mapping will be saved to the ARP cache of the network device. With the MAC address, the IP device can encapsulate DLL frames and send them to the LAN. By default, IP and ARP packets on the Ethernet are encapsulated in Ethernet II frames.

Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

2.2 Applications

Application	Description
LAN-based ARP	A user learns the MAC addresses of other users in the same network segment through ARP.
Proxy ARP-based Transparent Transmission	With Proxy ARP, a user can directly communicate with users in another network without knowing that it exists.

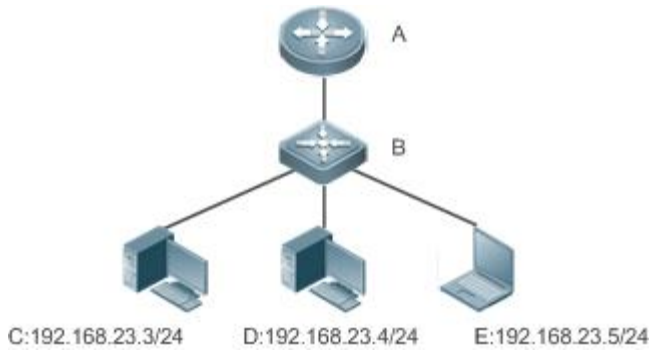
2.2.1 LAN-based ARP

Scenario

ARP is required in all IPv4 LANs.

- A user needs to learn the MAC addresses of other users through ARP to communicate with them.

Figure 2-1



Remarks	A is a router. B is a switch. It acts as the gateway. C, D, and E are hosts.

Deployment

- Enable ARP in a LAN to implement IP-MAC mapping.

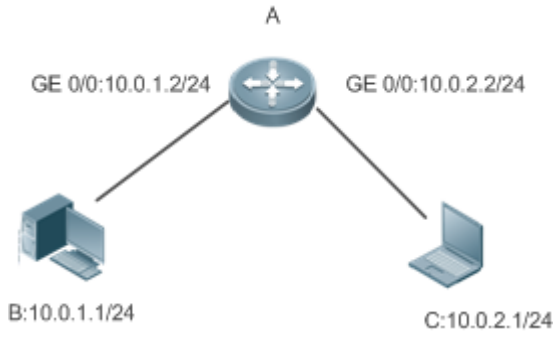
2.2.2 Proxy ARP-based Transparent Transmission

Scenario

Transparent transmission across IPv4 LANs is performed.

- Enable Proxy ARP on the router to achieve direct communication between users in different network segments.

Figure 2-2



Remarks	A is a router connecting two LANs. B and C are hosts in different subnets. No default gateway is configured for them.

Deployment

- Enable Proxy ARP on the subnet gateway. After configuration, the gateway can act as a proxy to enable a host without any route information to obtain MAC addresses of IP users in other subnets.

2.3 Features

Overview

Feature	Description
Static ARP	Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.
ARP Attributes	Users can specify the ARP entry timeout, ARP request retransmission times and interval, and maximum number of unresolved ARP entries.
Gratuitous ARP	Gratuitous ARP is used to detect IP address conflicts and enable peripheral devices to update ARP entries.
Proxy ARP	A proxy replies to the ARP requests from other devices in different subnets.
Local Proxy ARP	A proxy replies to the ARP requests from other devices in the same subnet.
ARP Trustworthiness Detection	Neighbor Unreachable Detection (NUD) is used to ensure that correct ARP entries are learned.
ARP-based IP Guard	You can set the number of IP packets for triggering ARP drop to prevent a large number of unknown unicast packets from being sent to the CPU.

2.3.1 Static ARP

Static ARP entries can be configured manually or assigned by the authentication server. The manually configured ones prevail. Static ARP can prevent the device from learning incorrect ARP entries.

Working Principle

If static ARP entries are configured, the device does not actively update ARP entries and these ARP entries permanently exist.

When the device forwards Layer-3 packets, the static MAC address is encapsulated in the Ethernet header as the destination MAC address.

Related Configuration

↘ Enabling Static ARP

Run the **arp** *ip-address mac-address type* command in global configuration mode to configure static ARP entries. By default, no static ARP entry is configured. ARP encapsulation supports only the Ethernet II type, which is represented by ARPA.

2.3.2 ARP Attributes

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.

Working Principle

↘ ARP Timeout

The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP entry timeout expires, the device sends a unicast ARP request packet to detect whether the peer end is online. If it receives an ARP reply from the peer end, it does not delete this ARP entry. Otherwise, the device deletes this ARP entry.

When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth.

↘ ARP Request Retransmission Interval and Times

The device consecutively sends ARP requests to resolve an IP address to a MAC address. The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request is retransmitted, the more likely the resolution will succeed and the more bandwidth ARP will consume.

Maximum Number of Unresolved ARP Entries

In a 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 users. To prevent such attacks, users can configure the maximum number of unresolved ARP entries.

Maximum Number of ARP Entries on an Interface

Configure the maximum number of ARP entries on a specified interface to prevent ARP entry resource waste.

Related Configuration

Configuring the ARP Timeout

Run the **arp timeout** *seconds* command in interface configuration mode to configure the ARP timeout. The default timeout is 3,600 seconds. You can change it based on actual situations.

Configuring the ARP Request Retransmission Interval and Times

- Run the **arp retry interval** *seconds* command in global configuration mode to configure the ARP request retransmission interval. The default interval is 1 second. You can change it based on actual situations.
- Run the **arp retry times** *number* command in global configuration mode to configure the ARP request retransmission times. The default number of retransmission times is 5. You can change it based on actual situations.

Configuring the Maximum Number of Unresolved ARP Entries

Run the **arp unresolve** *number* command in global configuration mode to configure the maximum number of unresolved ARP entries. The default value is the maximum number of ARP entries supported by the device. You can change it based on actual situations.

Configuring the Maximum Number of ARP Entries on an Interface

Run the **arp cache interface-limit** *limit* command in interface configuration mode to configure the maximum number of ARP entries learned on an interface. The default number is 0. You can change it based on actual situations. This command also applies to static ARP entries.

2.3.3 Gratuitous ARP

Working Principle

Gratuitous ARP packets are a special type of ARP packets. In a gratuitous ARP packet, the source and destination IP addresses are the IP address of the local device. Gratuitous ARP packets have two purposes:

4. IP address conflict detection. If the device receives a gratuitous packet and finds the IP address in the packet the same as its own IP address, it sends an ARP reply to notify the peer end of the IP address conflict.
5. ARP update. When the MAC address of an interface changes, the device sends a gratuitous ARP packet to notify other devices to update ARP entries.

The device can learn gratuitous ARP packets. After receiving a gratuitous ARP packet, the device checks whether the corresponding dynamic ARP entry exists. If yes, the device updates the ARP entry based on the information carried in the gratuitous ARP packet.

Related Configuration

Enabling Gratuitous ARP

Run the **arp gratuitous-send interval** *seconds* [*number*] command in interface configuration mode to enable gratuitous ARP. This function is disabled on interfaces by default. Generally you need to enable this function on the

gateway interface to periodically update the MAC address of the gateway on the downlink devices, which prevents others from faking the gateway.

2.3.4 Proxy ARP

Working Principle

The device enabled with Proxy ARP can help a host without any route information to obtain MAC addresses of IP users in other subnets. For example, if the device receiving an ARP request finds the source IP address in a different network segment 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. This is how Proxy ARP works.

Related Configuration

Enabling Proxy ARP

- Run the **ip proxy-arp** command in interface configuration mode to enable Proxy ARP.
- This function is enabled on routers while disabled on switches by default.

2.3.5 Local Proxy ARP

Working Principle

Local Proxy ARP means that a device acts as a proxy in the local VLAN (common VLAN or sub VLAN).

After local Proxy ARP is enabled, the device can help users to obtain the MAC addresses of other users in the same subnet. For example, when port protection is enabled on the device, users connected to different ports are isolated at Layer 2. After local Proxy ARP is enabled, the device receiving an ARP request acts as a proxy to send an ARP reply containing its own Ethernet MAC address. In this case, different users communicate with each other through Layer-3 routes. This is how local Proxy ARP works.

Related Configuration

Enabling Local Proxy ARP

- Run the **local-proxy-arp** command in interface configuration mode to enable local Proxy ARP.
- This function is disabled by default.
- This command is supported only on switch virtual interfaces (SVIs).

2.3.6 ARP Trustworthiness Detection

Working Principle

The **arp trust-monitor enable** command is used to enable anti-ARP spoofing to prevent excessive useless ARP entries from occupying device resources. After ARP trustworthiness detection is enabled on a Layer-3 interface, the device receives ARP request packets from this interface:

1. If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs NUD after 1 to 5 seconds. That is, the device begins to age the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer end within the aging time, it stores the entry. If not, it deletes the entry.
2. If the corresponding ARP entry exists, NUD is not performed.
3. If the MAC address in the existing dynamic ARP entry is updated, the device also performs NUD.

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, NUD is not required for learning and updating ARP entries.

Related Configuration

Enabling ARP Trustworthiness Detection

Run the **arp trust-monitor enable** command in interface configuration mode to enable ARP trustworthiness detection. This function is disabled by default.

2.3.7 ARP-based IP Guard

Working Principle

When receiving unresolved IP packets, the switch cannot forward them through the hardware and thereby need to send them to the CPU for address resolution. If a large number of such packets are sent to the CPU, the CPU will be congested, affecting other services on the switch.

After ARP-based IP guard is enabled, the switch receiving ARP request packets counts the number of packets in which the destination IP address hits this ARP entry. If this number is equal to the configured number, the switch sets a drop entry in the hardware so that the hardware will not send the packets with this destination IP address to the CPU. After the address resolution is complete, the switch continues to forward the packets with this destination IP address.

Related Configuration

Enabling ARP-based IP Guard

- Run the **arp anti-ip-attack** command in global configuration mode to configure the number of IP packets for triggering ARP drop.
- By default, the switch discards the corresponding ARP entry after it receives three unknown unicast packets containing the same destination IP address.

2.4 Configuration

Configuration	Description and Command	
Enabling Static ARP	(Optional) It is used to enable static IP-MAC binding.	
	arp	Enables static ARP.
Configuring ARP Attributes	(Optional) It is used to specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries and maximum number of ARP entries on an interface.	
	arp timeout	Configures the ARP timeout.
	arp retry interval	Configures the ARP request retransmission interval.
	arp unresolve	Configures the maximum number of unresolved ARP entries.
	arp cache interface-limit	Configures the maximum number of ARP entries on an interface.
Enabling Gratuitous ARP	(Optional) It is used to detect IP address conflicts and enables peripheral devices to update ARP entries.	
	arp gratuitous-send interval	Enables gratuitous ARP.
Enabling Proxy ARP	(Optional) It is used to act as a proxy to reply to ARP requests from the devices in different subnets.	
	ip proxy-arp	Enables Proxy ARP.

Configuration	Description and Command	
Enabling Local Proxy ARP	(Optional) It is used to act as a proxy to reply to ARP requests from other devices in the same subnet.	
	local-proxy-arp	Enables local Proxy ARP.
Enabling ARP Trustworthiness Detection	(Optional) It is used to unicast ARP request packets to ensure that correct ARP entries are learned.	
	arp trusted-monitor enable	Enables ARP trustworthiness detection.
Enabling ARP-based IP Guard	(Optional) It is used to prevent a large number of IP packets from being sent to the CPU.	
	arp anti-ip-attack	Configures the number of IP packets for triggering ARP drop.

2.4.1 Enabling Static ARP

Configuration Effect

Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.

Notes

After a static ARP entry is configured, the Layer-3 switch learns the physical port corresponding to the MAC address in the static ARP entry before it performs Layer-3 routing.

Configuration Steps

Configuring Static ARP Entries

- Optional.
- You can configure a static ARP entry to bind the IP address of the uplink device with its MAC address to prevent MAC change caused by ARP attacks.
- Configure static ARP entries in global configuration mode.

Verification

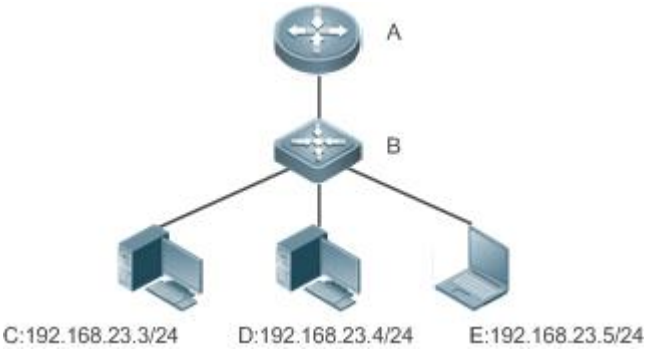
Run the **show running-config** command to check whether the configuration takes effect. Or run the **show arp static** command to check whether a static ARP cache table is created.

Related Commands

Configuring Static ARP Entries

Command	**arp** *ip-address mac-address type*
Parameter Description	*ip-address*: Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format. *mac-address*: Indicates the DLL address, consisting of 48 bits. *type*: Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.
Command Mode	Global configuration mode
Usage Guide	The system queries a 48-bit MAC address based on a 32-bit IP address in the ARP cache table. Since most hosts support dynamic ARP resolution, usually the static ARP mapping are not configured. Use the **clear arp-cache** command to delete the dynamic ARP entries.

Configuration Example

Scenario	
Configuration Steps	Configure a static ARP entry on B to statically bind the IP address of A with the MAC address. `Hostname(config)#arp 192.168.23.1 00D0.F822.334B arpa`

Verification	Run the **show arp static** command to display the static ARP entry.
	`Hostname(config)#show arp static`
	`Protocol Address Age(min) Hardware Type Interface`
	`Internet 192.168.23.1 <static> 00D0.F822.334B arpa`
	`1 static arp entries exist.`

Common Errors

- The MAC address in static ARP is incorrect.

2.4.2 Configuring ARP Attributes

Configuration Effect

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.

Configuration Steps

Configuring the ARP Timeout

- Optional.
- In a LAN, if a user goes online/offline frequently, it is recommended to set the ARP timeout small to delete invalid ARP entries as soon as possible.
- Configure the ARP timeout in interface configuration mode.

Configuring the ARP Request Retransmission Interval and Times

- Optional.
- If the network resources are insufficient, it is recommended to set the ARP request retransmission interval great and the retransmission times small to reduce the consumption of network bandwidths.
- Configure the ARP request retransmission interval and times in global configuration mode.

Configuring the Maximum Number of Unresolved ARP Entries

- Optional.

- If the network resources are insufficient, it is recommended to set the maximum number of unresolved ARP entries small to reduce the consumption of network bandwidths.
- Configure the maximum number of unresolved ARP entries in global configuration mode.

Configuring the Maximum Number of ARP Entries on an Interface

- Optional.
- Configure the maximum number of ARP entries on an interface in interface configuration mode.

Verification

Run the **show arp timeout** command to display the timeouts of all interfaces.

Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.

Related Commands

Configuring the ARP Timeout

Command	**arp timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout in seconds, ranging from 0 to 2,147,483. The default value is 3,600.
Command Mode	Interface configuration mode
Usage Guide	The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. Unless otherwise specified, do not configure the ARP timeout.

Configuring the ARP Request Retransmission Interval and Times

Command	**arp retry interval** *seconds*
Parameter Description	*seconds*: Indicates the ARP request retransmission interval in seconds, ranging from 1 to 3,600. The default value is 1.
Command Mode	Global configuration mode
Usage Guide	If a device frequently sends ARP requests, affecting network performance, you can set the ARP request retransmission interval longer. Ensure that this interval does not exceed the ARP timeout.

Configuring the Maximum Number of Unresolved ARP Entries

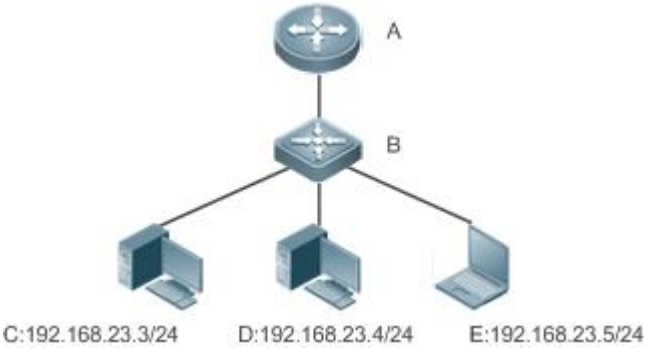
Command	**arp unresolve** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ARP entries, ranging from 1 to 1,000. The default value is 1,000.
Command Mode	Global configuration mode

Usage Guide	If a large number of unresolved entries exist in the ARP cache table and remain in the table after a while, it is recommended to use this command to limit the number of unresolved ARP entries.

Configuring the Maximum Number of ARP Entries on an Interface

Command	**arp cache interface-limit** *limit*
Parameter Description	*limit*: Indicates the maximum number of ARP entries that can be learned on an interface, including configured ARP entries and dynamically learned ARP entries. The value ranges from 0 to 512. 0 indicates no limit on this number.
Command Mode	Interface configuration mode
Usage Guide	Limiting the number of ARP entries on an interface can prevent malicious ARP attacks from generating excessive ARP entries on the device and occupying entry resources. 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.

Configuration Example

Scenario	
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users
Configuration Steps	● Set the ARP timeout to 60 seconds on port GigabitEthernet 0/1. ● Set the maximum number of learned ARP entries to 300 on port GigabitEthernet 0/1. ● Set the ARP request retransmission interval to 3 seconds. ● Set the ARP request retransmission times to 4. ● Set the maximum number of unresolved ARP entries to 4,096. ● Set the maximum number of learned ARP entries to 1,000 on Sub Slot 2 of Slot 1.

	`Hostname(config)#interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#arp timeout 60`
	`Hostname(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300`
	`Hostname(config-if-GigabitEthernet 0/1)#exit`
	`Hostname(config)#arp retry interval 3`
	`Hostname(config)#arp retry times 4`
	`Hostname(config)#arp unresolve 4096`

Verific	● Run the **show arp timeout** command to display the timeout of the interface.

ation	● Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries and maximum number of ARP entries on the interface.
	Hostname#show arp timeout Interface arp timeout(sec) ---------- ---------- GigabitEthernet 0/1 60 GigabitEthernet 0/2 3600 GigabitEthernet 0/4 3600 GigabitEthernet 0/5 3600 GigabitEthernet 0/7 3600 VLAN 100 3600 VLAN 111 3600 Hostname(config)# show running-config arp unresolve 4096 arp retry times 4 arp retry interval 3 ! interface GigabitEthernet 0/1 arp cache interface-limit 300

2.4.3 Enabling Gratuitous ARP

Configuration Effect

The interface periodically sends gratuitous ARP packets.

Configuration Steps

- Optional.
- When a switch acts as the gateway, enable gratuitous ARP on an interface to prevent other users from learning incorrect gateway MAC address in case of ARP spoofing.
- Enable gratuitous ARP in interface configuration mode.

Verification

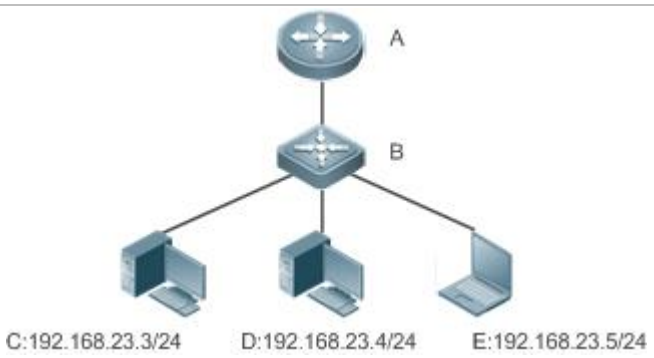
Run the show running-config interface [*name*] command to check whether the configuration is successful.

Related Commands

↘ Enabling Gratuitous ARP

Command	**arp gratuitous-send interval** *seconds* [*number*]
Parameter Description	*seconds*: Indicates the interval for sending a gratuitous ARP request. The unit is second. The value ranges from 1 to 3,600. *number*: Indicates the number of gratuitous ARP requests that are sent. The default value is 1. The value ranges from 1 to 100.
Command Mode	Interface configuration mode
Usage Guide	If a network interface of a device acts as the gateway for downstream devices but a downstream device pretends to be the gateway, enable gratuitous ARP on the interface to advertise itself as the real gateway.

Configuration Example

Scenario	
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users
Configuration Steps	Configure the GigabitEthernet 0/0 interface to send a gratuitous ARP packet every 5 seconds.
	`Hostname(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5`
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.

	`Hostname#sh running-config interface gigabitEthernet 0/0`
	
	`Building configuration...`
	`Current configuration : 127 bytes`
	`!`
	`interface GigabitEthernet 0/0`
	` duplex auto`
	` speed auto`
	` ip address 30.1.1.1 255.255.255.0`

	arp gratuitous-send interval 5

2.4.4 Enabling Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users.

Notes

By default, Proxy ARP is disabled on Layer-3 switches.

Configuration Steps

- Optional.
- If a user without any route information needs to obtain the MAC addresses of the IP users in other subnets, enable Proxy ARP on the device so that the device can act as a proxy to send ARP replies.
- Enable Proxy ARP in interface configuration mode.

Verification

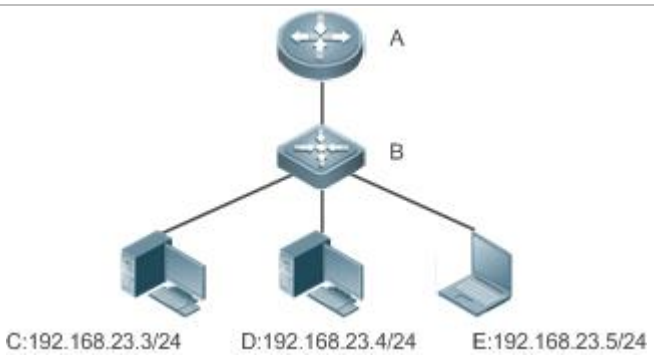
Run the **show ip interface** [*name*] command to check whether the configuration takes effect.

Related Commands

Enabling Proxy ARP

Command	**ip proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users

Configuration Steps	Enable Proxy ARP on port GigabitEthernet 0/0.
	`Hostname(config-if-GigabitEthernet 0/0)#ip proxy-arp`
Verification	Run the **show ip interface** command to check whether the configuration takes effect.

	`Hostname#show ip interface gigabitEthernet 0/0`
	`GigabitEthernet 0/0`
	`  IP interface state is: DOWN`
	`  IP interface type is: BROADCAST`
	`  IP interface MTU is: 1500`
	`  IP address is:`
	`    No address configured`
	`  IP address negotiate is: OFF`
	`  Forward direct-broadcast is: OFF`
	`  ICMP mask reply is: ON`
	`  Send ICMP redirect is: ON`
	`  Send ICMP unreachable is: ON`
	`  DHCP relay is: OFF`
	`  Fast switch is: ON`
	`  Help address is: 0.0.0.0`
	`  Proxy ARP is: ON`
	`ARP packet input number: 0`
	`  Request packet     : 0`
	`  Reply packet       : 0`
	`  Unknown packet     : 0`
	`TTL invalid packet number: 0`
	`ICMP packet input number: 0`
	` Echo request       : 0`
	` Echo reply         : 0`
	` Unreachable        : 0`
	` Source quench      : 0`
	` Routing redirect   : 0`

2.4.5 Enabling Local Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users in the same subnet.

Notes

Local Proxy ARP is supported only on SVIs.

Configuration Steps

- Optional.
- If a user enabled with port protection needs to communicate with users in the VLAN, enable local Proxy ARP on the device.
- Enable local Proxy ARP in interface configuration mode.

Verification

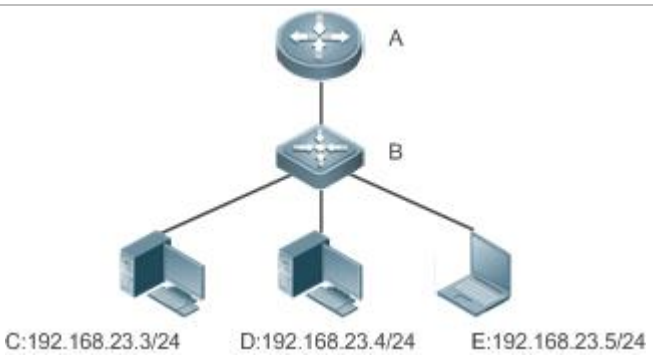
Run the **show running-config interface** [*name*] command to check whether the configuration takes effect.

Related Commands

Enabling Local Proxy ARP

Command	**local-proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users
Configuration Steps	Enable local Proxy ARP on the VLAN 1 interface.

	Hostname(config-if-VLAN 1)#local-proxy-arp
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Hostname#show running-config interface vlan 1 Building configuration... Current configuration : 53 bytes interface VLAN 1 ip address 192.168.1.2 255.255.255.0 local-proxy-arp

2.4.6 Enabling ARP Trustworthiness Detection

Configuration Effect

Enable ARP trustworthiness detection. If the device receiving an ARP request packet fails to find the corresponding entry, it performs NUD. If the MAC address in the existing dynamic ARP entry is updated, the device immediately performs NUD to prevent ARP attacks.

Notes

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

Configuration Steps

- Optional.
- If there is a need for learning ARP entries, enable ARP trustworthiness detection on the device. If the device receiving an ARP request packet fails to find the corresponding entry, it needs to send a unicast ARP request packet to check whether the peer end exists. If yes, the device learns the ARP entry. If not, the device does not learn the ARP entry. If the MAC address in the ARP entry changes, the device will immediately perform NUD to prevent ARP spoofing.
- Enable ARP trustworthiness detection in interface configuration mode.

Verification

Run the **show running-config interface** [*name*] command to check whether the configuration take effect

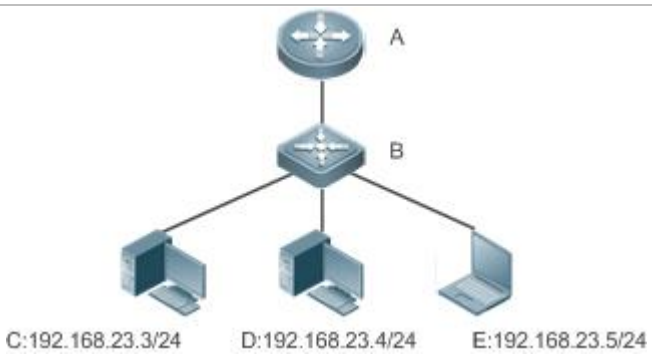
Related Commands

Enabling ARP Trustworthiness Detection

Command	**arp trust-monitor enable**
Parameter Description	N/A

Command Mode	Interface configuration mode
Usage Guide	Enable this function. If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD. Enable this function. If the MAC address of the existing dynamic ARP entry is updated, the device immediately performs NUD. After this function is disabled, the device does not perform NUD for learning or updating ARP entries.

Configuration Example

Scenario	
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users
Configuration Steps	Enable ARP trustworthiness detection on port GigabitEthernet 0/0.
	`Hostname(config-if-GigabitEthernet 0/0)#arp trust-monitor enable`
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.

	`Hostname#show running-config interface gigabitEthernet 0/0`
	
	`Building configuration...`
	`Current configuration : 184 bytes`
	`!`
	`interface GigabitEthernet 0/0`
	` duplex auto`
	` speed auto`
	` ip address 30.1.1.1 255.255.255.0`
	` arp trust-monitor enable`

2.4.7 Enabling ARP-based IP Guard

Configuration Effect

When the CPU receives the specified number of packets in which the destination IP address hits the ARP entry, all packets with this destination IP address will not be sent to the CPU afterwards.

Notes

ARP-based IP guard is supported on switches.

Configuration Steps

- Optional.
- By default, when three unknown unicast packets are sent to the switch CPU, the drop entry is set. Users can run this command to adjust the number of packets for triggering ARP drop based on the network environment. Users can also disable this function.
- Configure ARP-based IP guard in global configuration mode.

Verification

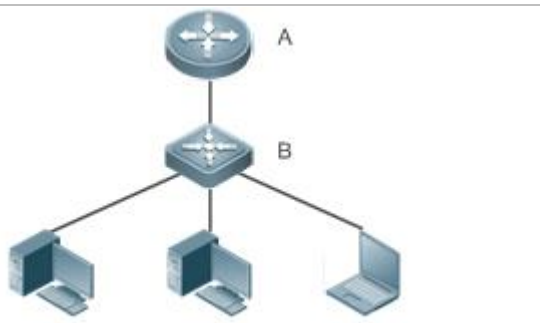
Run the **show run** command to check whether the configuration takes effect.

Related Commands

Enabling ARP-based IP Guard

Command	**arp anti-ip-attack** *num*
Parameter Description	*num*: Indicates the number of IP packets for triggering ARP drop. The value ranges from 0 to 100. 0 indicates that ARP-based IP guard is disabled. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	If hardware resources are sufficient, run the **arp anti-ip-attack** *num* command to set the number of IP packets for triggering ARP drop to a small value. If hardware resources are insufficient, run the **arp anti-ip-attack** *num* command to set the number of IP packets for triggering ARP drop to a large value, or disable this function.

Configuration Example

Scenario	
Remarks	A: Router B: Switch serving as a gateway

	C, D and E: Users
Configuration Steps	Enable ARP-based IP guard on B. `Hostname(config)#arp anti-ip-attack 10`
Verification	Run the **show running-config** command to check whether the configuration takes effect.

	`Hostname#show running-config`
	
	`Building configuration...`
	`Current configuration : 53 bytes`
	`arp anti-ip-attack 10`

2.5 Monitoring

Clearing

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

Description	Command
Clears dynamic ARP entries. In gateway authentication mode, dynamic ARP entries in authentication VLANs are not cleared.	**clear arp-cache**

Displaying

Description	Command
Displays the ARP table in detail.	**show arp** [**detail**] [*interface-type interface-number*[*ip* [*mask*] | *mac-address* | **static**| **complete** | **incomplete**]]
Displays the ARP table.	**show ip arp**
Displays the ARP entry counter.	**show arp counter**
Displays the timeout of dynamic ARP entries.	**show arp timeout**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ARP packet sending and receiving.	**debug arp**
Debugs the creation and deletion of ARP entries.	**debug arp event**

3 Configuring IPv6

3.1 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), which is described in RFC 2460.

Note:

"Router" in this chapter refers to the network device that supports the routing function. These network devices can be Layer 3 switches, routers, firewalls, etc.

Main Features

Larger Address Space

Compared with 32 bits in an IPv4 address, the length of an IPv6 address is extended to 128 bits. Therefore, the address space has approximately 2^{128} addresses. IPv6 adopts a hierarchical address allocation mode to support address allocation of multiple subnets from the Internet core network to intranet subnet.

Simpler Packet Header Format

Since the design principle of the IPv6 packet header is to minimize the overhead of the packet header, some non-key fields and optional fields are removed from the packet header to the extended packet header. Therefore, although the length of an IPv6 address is four times of that of an IPv4 address, the IPv6 packet header is only two times of the IPv4 packet header. The IPv6 packet header makes device forwarding more efficient. For example, with no checksum in the IPv6 packet header, the IPv6 device does not need to process fragments (fragmentation is completed by the initiator).

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 as a uniform network prefix on the upstream device, greatly reducing routing entries maintained by the device and routing and storage overheads 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), MTU Discovery, Router Advertisement (RA), Router Solicitation (RS), and auto-configuration technologies provide related services for PnP. Particularly, IPv6 offers two types of auto-configuration: stateful auto-configuration and stateless auto-configuration. In IPv4, Dynamic Host Configuration Protocol (DHCP) realizes auto-configuration of the host IP address and related parameters. IPv6 inherits this auto-configuration service from IPv4 and called it stateful auto-configuration (see DHCPv6). Besides, IPv6 also offers the stateless auto-configuration service. During stateless auto-configuration, a host automatically obtains the local address of the link, address prefix of the local device, and other related configurations.

Security

As an optional extension protocol of IPv4, Internet Protocol Security (IPSec) is a part of IPv6 to provide security for IPv6 packets. At present, IPv6 provides two mechanisms: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH provides data integrity and authenticates IP packet sources to ensure that the packets originate 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 flow. Using this field, IPv6 allows users to propose requirements on the communication quality. , 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 neighboring nodes (nodes on the same link). IPv6 uses NDP packets and efficient multicast/unicast ND packets instead of broadcast-based Address Resolution Protocol (ARP) and Control Message Protocol Version 4 (ICMPv4) router discovery packets.

Extensibility

With strong extensibility, IPv6 features can be added to the extended packet header following the IPv6 packet header. Unlike IPv4, the IPv6 packet header can support at most 40 bytes of options. For an IPv6 packet, the length of the extended packet header is restricted only by the maximum number of bytes in the packet.

Protocols and Standards

- RFC 4291 - IP Version 6 Addressing Architecture
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 - IPv6 Stateless Address Auto-configuration
- RFC 5059 - Deprecation of Type 0 Routing Headers in IPv6

3.2 Applications

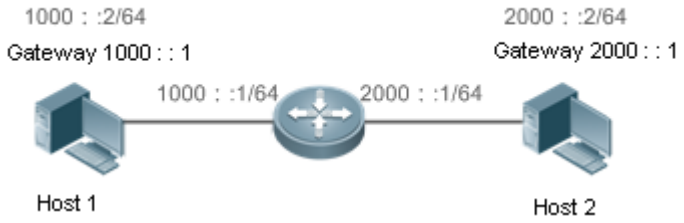
Application	Description
Communication Based on IPv6 Addresses	Two PCs communicate with each other using IPv6 addresses.

3.2.1 Communication Based on IPv6 Addresses

Scenario

As shown in Figure 3-1, Host 1 and Host 2 communicate with each other using IPv6 addresses.

Figure 3-1



Deployment

Hosts can use the stateless address auto-configuration or DHCPv6 address assignment mode. After addresses are configured, hosts can communicate with each other using IPv6 addresses.

3.3 Features

Overview

Feature	Description
IPv6 Address Format	The IPv6 address format makes IPv6 have a larger address space and flexible representation approach.
IPv6 Address Type	IPv6 identifies network applications based on addresses.
IPv6 Packet Header Format	IPv6 simplifies the fixed and extended packet headers to improve the data packet processing and forwarding efficiency of the device.
IPv6 Neighbor Discovery	ND 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.
IPv6 Source Routing	This feature is used to specify the intermediate nodes that a packet passes through along the path to the destination address. It is similar to the IPv4 loose source routing option and loose record routing option.
Restricting the Sending Rate of ICMPv6 Error Messages	This feature prevents DoS attacks.
IPv6 HOP-LIMIT	This feature prevents useless unicast packets from being unlimitedly transmitted on the network and wasting network bandwidth.

3.3.1 IPv6 Address Format

An IPv6 address is represented in the X:X:X:X:X:X:X:X format, where X is a 4-digit hexadecimal integer (16 bits). Each address consists of 8 integers, with a total of 128 bits (each integer contains 4 hexadecimal digits and each digit contains four bits). 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

These integers are hexadecimal, where A to F represent 10 to 15. Each integer in the address must be represented, except the leading zeroes in each integer. If an IPv6 address contains a string of zeroes (as shown in the second and third examples above), a double colon (::) can be used to represent these zeroes. That is, 800:0:0:0:0:0:0:1 can be represented as 800::1.

A double colon indicates that this address can be extended to a complete 128-bit address. In this approach, only when the 16-bit integers are all 0s, can they can be replaced with a double colon. A double colon can exist once in an IPv6 address.

In IPv4/IPv6 mixed environment, an address has a mixed representation. 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 mixed manner, that is, X:X:X:X:X:X:d.d.d.d, where X is a hexadecimal integer and d is a 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. Typical applications are IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. If the first 96 bits are 0 in an IPv4-compatible IPv6 address, this address can be represented as ::A.B.C.D, e.g., ::1.1.1.1. IPv4-compatible addresses have been abolished at present. IPv4-mapped IPv6 addresses are represented as ::FFFF:A.B.C.D to represent IPv4 addresses as IPv6 addresses. For example, IPv4 address 1.1.1.1 mapped to an IPv6 address is represented as ::FFFF:1.1.1.1.

Since an IPv6 address is divided into two parts: subnet prefix and interface ID, it can be represented as an address with an additional value according to an address allocation method like Classless Inter-Domain Routing (CIDR). The additional value indicates how many bits (subnet prefix) in the address represent the network part. That is, the IPv6 node address contains the prefix length. The prefix length is separated from the IPv6 address by a slash. For example, in 12AB::CD30:0:0:0:0/60, the prefix length used for routing is 60 bits.

Related Configuration

Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure an IPv6 address on an interface.
- After configuration, a host can communicate with others using the configured IPv6 address based on DAD.

3.3.2 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 interface included in this address (the nearest interface according to the routing protocol).

IPv6 does not define broadcast addresses.

These three types of addresses are described as follows:

Unicast Addresses

Unicast addresses fall into five types: unspecified address, loopback address, link-local address, site-local address, and global unicast address. At present, site-local addresses have been abolished. Except unspecified, loopback, and link-local addresses, all other addresses are global unicast addresses.

- Unspecified address

The unspecified address is 0:0:0:0:0:0:0:0, which is usually abbreviated to ::. It has two general purposes:

1. 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.
2. 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 free ARP packet).

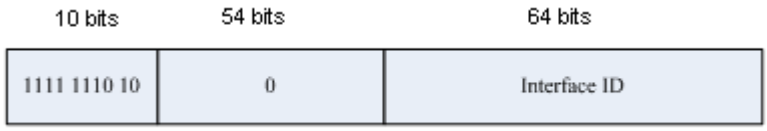
- Loopback address

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 itself packets.

- Link-local address

The format of a link-local address is as follows:

Figure 3-2

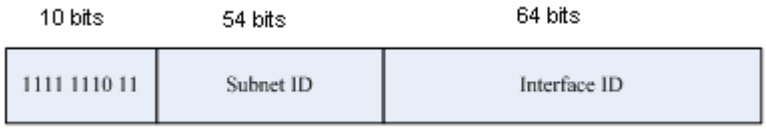


The link-local address is used on a single network link to assign IDs to hosts. The address identified by the first 10 bits in the prefix is the link-local address. A device never forwards packets in which the source or destination address contains the link-local address. The intermediate 54 bits in the address are all 0s. The last 64 bits represent the interface ID, which allows a single network to connect 2^{64}-1 hosts.

- Site-local address

The format of a site-local address is as follows:

Figure 3-3

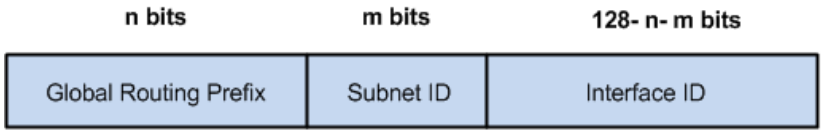


A site-local address is used to transmit data within a site. A device never forwards packets in which the source or destination address contains the site-local address to the Internet. That is, these packets can be forwarded only within the site. A site can be assumed as an enterprise's local area network (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 the first 10 bits as the prefix and are all regarded as global unicast addresses. Existing addresses can continue to use this prefix.

- Global unicast address

The format of a global unicast address is as follows:

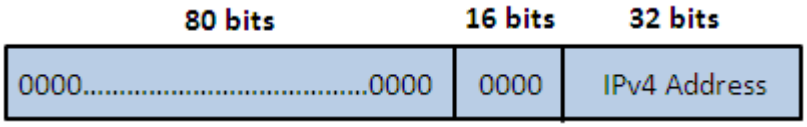
Figure 3-4



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.

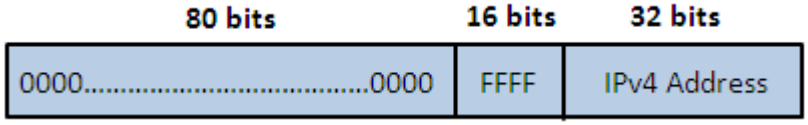
The format of an IPv4-compatible IPv6 address is as follows:

Figure 3-5



The format of an IPv4-mapped IPv6 address is as follows:

Figure 3-6



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 the 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.

Multicast Addresses

The format of an IPv6 multicast address is as follows:

```
|    8     |  4 |  4 |                   112 bits                   |
+--------+----+----+----------------------------------------------+
|11111111|flgs|scop|                   group ID                   |
+--------+----+----+----------------------------------------------+
```

The first byte in the address is all 1s, representing a multicast address.

- Flag field

The flag field consists of four bits. Currently only the fourth bit is specified to indicate whether this address is a known multicast address assigned by the Internet Assigned Numbers Authority (IANA) or a temporary multicast address in a

certain scenario. If the flag bit is 0, this address is a known multicast address. If the flag bit is 1, this address is a temporary multicast address. The remaining three flag bits are reserved for future use.

- Scope field

The scope field consists of four bits to indicate the multicast range. That is, a multicast group includes the local node, local link, local site, and any node in the IPv6 global address space.

- Group ID field

The group ID consists of 112 bits to identify a multicast group. A multicast ID can represent different groups based on the flag and scope fields.

IPv6 multicast addresses are prefixed with FF00::/8. 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. For a node (host or device), you must add the following multicast addresses:

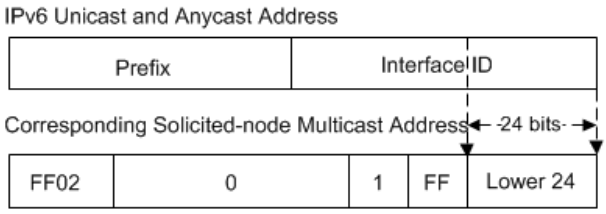
3. Multicast address for all nodes on the local link, that is, FF02::1
4. Solicited-node multicast address, prefixed with FF02:0:0:0:0:1:FF00:0000/104

If the node is a device, it also has to be added to the multicast address of all devices on the local link, that is, FF02::2.

The solicited-node multicast address corresponds to the IPv6 unicast and anycast address. You must add a corresponding solicited-node multicast address for each configured unicast and anycast address of an IPv6 node. The solicited-node multicast address is prefixed with FF02:0:0:0:0:1:FF00:0000/104. The remaining 24 bits are composed of the least significant 24 bits of the unicast or anycast address. For example, if the unicast address is FE80::2AA:FF:FE21:1234, the solicited-node multicast address is FF02::1:FF21:1234.

The solicited-node multicast address is usually used in NS packets. Its address format is as follows:

Figure 3-7



Anycast Addresses

Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node in the anycast address receives data packets while all nodes included in the multicast address receive data packets. Since anycast addresses are allocated to the normal IPv6 unicast address space, they have the same formats with unicast addresses. Every member in an anycast address must be configured explicitly for easier recognition.

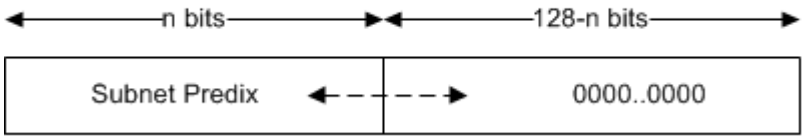
Anycast addresses can be allocated only to devices and cannot be used as source addresses of packets.

RFC 2373 redefines an anycast address called subnet-router anycast address. Figure 3-8 shows the format of a subnet-router anycast address. Such an address consists of the subnet prefix and a series of 0s (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 3-8

Format of a Subnet-router Anycast Address



Related Configuration

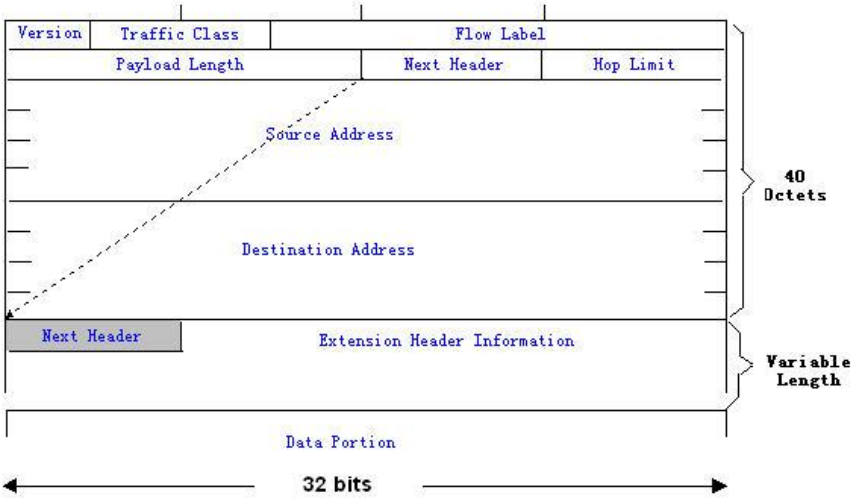
Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure the IPv6 unicast address and anycast address of an interface.
- After an interface goes up, it will automatically join the corresponding multicast group.

3.3.3 IPv6 Packet Header Format

Figure 3-9 shows the format of the IPv6 packet header.

Figure 3-9



The IPv4 packet header is in unit of four bytes. The IPv6 packet header consists of 40 bytes, in unit of eight bytes. The 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 by this packet, similar to the 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 Tx source of multiple service flows. The flow label and source 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 TCP or UDP. It can also be used to indicate existence of the IPv6 extension header.

- Hop Limit

This field consists of 8 bits. Every time a device forwards a packet, the field value reduced by 1. If the field 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 (Type 0 routing header)

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 the 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 the IPv6 packet header receives a 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 routing header list 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

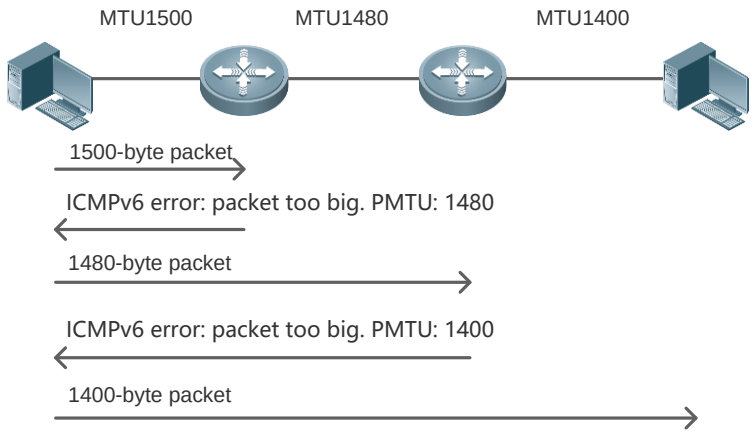
This extension header indicates the protocol used at the upper layer, such as TCP (6) and UDP (17).

Another two extension headers AH and ESP will be described in the *Configuring IPSec*.

3.3.4 IPv6 PMTU Discovery

Similar to IPv4 PMTU discovery, IPv6 PMTUD allows a host to dynamically discover and adjust the MTU size on the data Tx path. If the length of a data packet to be sent by a host is greater than the PMTU, the host performs packet fragmentation on its own. In this manner, the IPv6 device does not need to perform fragmentation, saving device resources and improving the IPv6 network efficiency.

Figure 3-1



As shown in the Figure 3-2, if the length of a packet to be sent by the 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 then 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.

Related Configuration

Configuring IPv6 MTU on an interface

- The default IPv6 MTU is 1500 on an Ethernet interface.
- Run the **ipv6 mtu** command to modify the IPv6 MTU of an interface.

3.3.5 IPv6 Neighbor Discovery

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, NUD, DAD, and redirection. NDP defines five ICMP packets: RS (ICMP type: 133), RA (ICMP type: 134), NS (similar to ARP request, ICMP type: 135), NA (similar to ARP reply, ICMP type: 136), ICMP Redirect (ICMP type: 137).

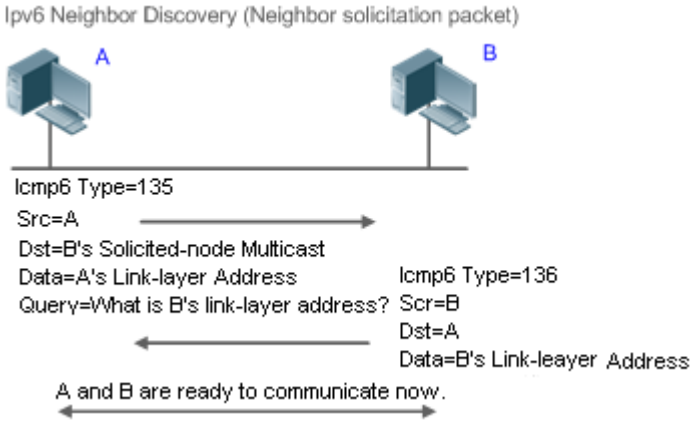
All the above ICMP packets carry one or multiple options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: Source Link-Layer Address Option, Type=1; Target Link-Layer Address Option, Type=2; Prefix Information Option, Type=3; Redirection Header Option, Type=4; MTU Option, Type=5.

Address Resolution

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer end by sending it an NS packet. 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 peer end replies with an NA packet in which the destination address is the source address of the NS packet, that is, the link-layer address of the solicited node. After receiving this NA packet, the source node can communicate with the destination node.

Figure 3-11 shows the address resolution process.

Figure 3-11



NUD

If the reachable time of a neighbor has elapsed but an IPv6 unicast packet needs to be sent to it, the device performs NUD.

While performing NUD, the device can continue to forward IPv6 packets to the neighbor.

DAD

To know whether the IPv6 address configured for a host is unique, the device needs to perform DAD by sending an NS packet in which the source IPv6 address is the unspecified address.

If a device detects an address conflict, this address is set to the duplicate status so that the device cannot receive IPv6 packets with this address being the destination address. Meanwhile, the device also starts a timer for this duplicate address to periodically perform DAD. If no address conflict is detected in re-detection, this address can be properly used.

Router, Prefix, and Parameter Discovery

A device periodically sends RA packets to all local nodes on the link.

The following figure shows the RA packet sending process.

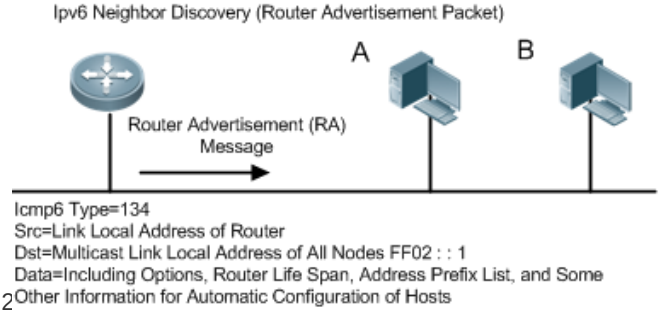


Figure 3-12

An RA packet usually contains the following content:

- One or multiple IPv6 address prefixes (used for on-link determination or stateless address auto-configuration)
- Validity 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 interval 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 started rather than wait for the RA packets sent by the device. If no

unicast address is configured for a newly started host, the host includes the unspecified address (0:0:0:0:0:0:0:0) as the source address in the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all local routing devices (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 local nodes (FF02::1).

In an RA packet, the following parameters can be configured:

- Ra-interval: Interval for sending the RA packet.
- Ra-lifetime: Lifetime of a router, that is, whether the device acts as the default router on the local link and the interval for acting as the default router.
- Prefix: Prefix of an IPv6 address on 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: NS packet retransmission interval.
- Reachabletime: Period when the device regards a neighbor reachable after detecting a Confirm Neighbor Reachability event.
- Ra-hoplimit: Hops of the RA packet, used to set the hop limit for a host to send a unicast packet.
- Ra-mtu: MTU of the RA packet.
- Managed-config-flag: Whether a host receiving this RA packet obtains the address through stateful auto-configuration.
- Other-config-flag: Whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

Configure the above parameters when configuring IPv6 interface attributes.

Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends the 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.

Maximum Number of Unresolved ND Entries

- You can configure the maximum number of unresolved ND entries to prevent malicious scanning network segments from generating a large number of unresolved ND entries and occupying excessive memory space.

Maximum Number of Neighbor Learning Entries on an Interface

- You can configure the maximum number of neighbor learning entries on an interface to prevent neighbor learning attacks from occupying ND entries and memory space of the device and affecting forwarding efficiency of the device.

Related Configuration

Enabling IPv6 Redirection

- By default, ICMPv6 Redirect packets can be sent on IPv6 interfaces.
- Run the **no ipv6 redirects** command in interface configuration mode to prohibit an interface from sending Redirect packets.

Configuring IPv6 DAD

- By default, an interface sends one NS packet to perform IPv6 DAD.
- Run the **ipv6 nd dad attempts** *value* command in interface configuration mode to configure the number of NS packets consecutively sent by DAD. Value 0 indicates disabling DAD for IPv6 addresses on this interface.
- Run the **no ipv6 nd dad attempts** command to restore the default configuration.
- By default, the device performs DAD on duplicate IPv6 addresses every 60 seconds.
- Run the **ipv6 nd dad retry** value command in global configuration mode to configure the DAD interval. Value 0 indicates disabling DAD for the device.

- Run the **no ipv6 nd dad retry** command to restore the default configuration.

Configuring the Reachable Time of a Neighbor

- The default reachable time of an IPv6 neighbor is 30s.
- Run the **ipv6 nd reachable-time** *milliseconds* command in interface configuration mode to modify the reachable time of a neighbor.

Configuring the Stale Time of a Neighbor

- The default stale time of an IPv6 neighbor is 1 hour. After the time elapses, the device performs NUD.
- Run the **ipv6 nd stale-time** *seconds* command in interface configuration mode to modify the stale time of a neighbor.

Configuring Prefix Information

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.
- Run the **ipv6 nd prefix** command in interface configuration mode to add or delete prefixes and prefix parameters that can be advertised.

Enabling/disabling RA Suppression

- By default, an IPv6 interface does not send RA packets.
- Run the **no ipv6 nd suppress-ra** command in interface configuration mode to disable RA suppression.

Configuring the Maximum Number of Unresolved ND Entries

- The default value is 0, indicating no restriction. It is only restricted to the ND entry capacity supported by the device.
- Run the **ipv6 nd unresolved** *number* command in global configuration mode to restrict the number of unresolved neighbors. After the entries exceed this restriction, the device does not actively resolve subsequent packets.

Configuring the Maximum Number of ND Entries Learned on an Interface

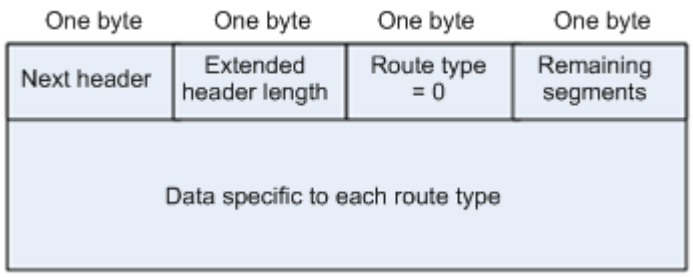
- Run the **ipv6 nd cache interface-limit** *value* command in interface configuration mode to restrict the number of neighbors learned on an interface. The default value is 0, indicating no restriction.

3.3.6 IPv6 Source Routing

Working Principle

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 along the path to the destination address. It uses the following format:

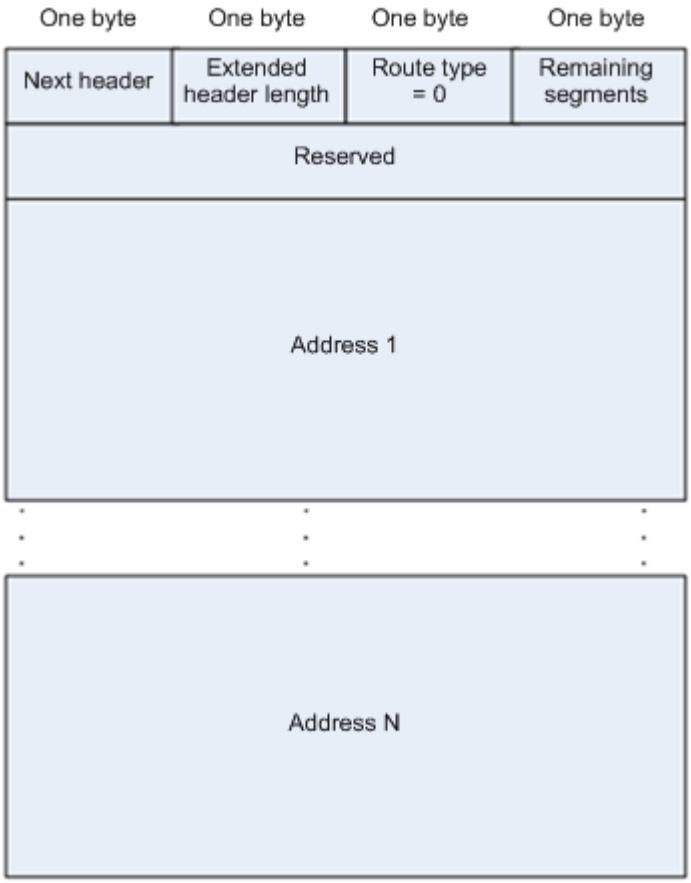
Figure 3-13



The Segments Left field is used to indicate how many intermediate nodes are specified in the routing header for the packet to pass through from the current node to the final destination address.

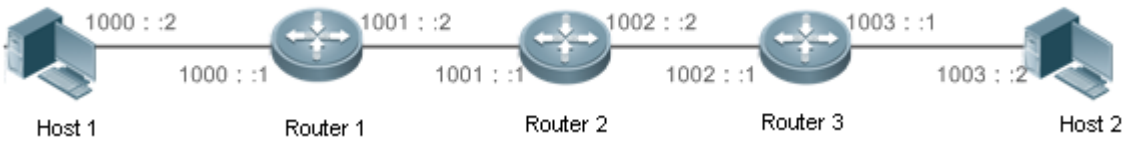
Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. RFC 2460 defines the Type 0 routing header (similar to the loose source routing option of IPv4). The format of the Type 0 routing header is as follows:

Figure 3-14



The following example describes the application of the Type 0 routing header, as shown in Figure 3-15.

Figure 3-15



Host 1 sends Host 2 a packet specifying the intermediate nodes Router 2 and Router 3. The following table lists the changes of fields related to the IPv6 header and routing header during the forwarding process.

Transmission Node	Fields in the IPv6 Header	Fields Related to the Type 0 Routing Header
Host 1	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 1	No change	
Router 2	Source address=1000::2	Segments Left=1

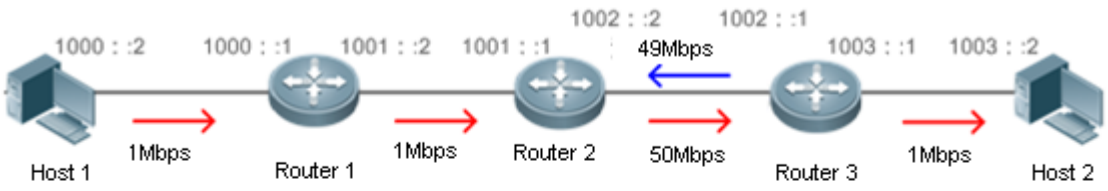
	Destination address=1002::1 (Address of Router 3)	Address 1=1001::1 (Address of Router 2) Address 2=1003::2 (Address of Host 2)
Router 3	Source address=1000::2 Destination address=1003::2 (Address of Host 2)	Segments Left=0 Address 1=1001::1 (Address of Router 2) Address 1=1002::2 (Address of Router 3)
Host 2	No change	

The forwarding process is as follows:

5. Host 1 sends a packet in which the destination address is Router 2's address 1001::1, the Type 0 routing header is filled with Router 3's address 1002::1 and Host 2's address 1003::2, and the value of the Segments Left field is 2.
6. Router 1 forwards this packet to Router 2.
7. Router 2 changes the destination address in the IPv6 header to Address 1 in the routing header. That is, the destination address becomes Router 3's address 1002::1, Address 1 in the routing header becomes Router 2's address 1001::1, and the value of the Segments Left field becomes 1. After modification, Router 2 forwards the packet to Router 3.
8. Router 3 changes the destination address in the IPv6 header to Address 2 in the routing header. That is, the destination address becomes Host 2's address 1003::2, Address 2 in the routing header becomes Router 3's address 1002::1, and the value of the Segments Left field becomes 0. After modification, Router 3 forwards the packet to Host 2.

The Type 0 routing header may be used to initiate DoS attacks. As shown in Figure 3-16, Host 1 sends packets to Host 2 at 1 Mbps and forges a routing header to cause multiple round-trips 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 3-16



IPv6 Packet
Source Address 1000::2
Destination Address 1001:1

Segments Left in the Type 0 Routing Header: 100
Address 1: 1002::1
Address 2: 1001::1
Address 3: 1002::1
Address 4: 1002::1
...
Address 99: 1002::1
Address 100: 100:3::2

Host 1 sends packets to Host 2, passing through Router 2, Router 3, Router 2, and Router 3, ...
Each packet is sent 50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2.

Related Configuration

Enabling IPv6 Source Routing

- The Type 0 routing header is not supported by default.
- Run the **ipv6 source-route** command in global configuration mode to enable IPv6 source routing.

3.3.7 Restricting the Sending Rate of ICMPv6 Error Messages

Working Principle

The destination node or intermediate router sends ICMPv6 error messages to report the errors incurred during IPv6 data packet forwarding and transmission. There are mainly four types of error messages: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

When receiving an invalid IPv6 packet, a device discards the packet and sends back an ICMPv6 error message to the source IPv6 address. In the case of invalid IPv6 packet attacks, the device may continuously reply to ICMPv6 error messages till device resources are exhausted and thereby fail to properly provide services. To solve this problem, you can restrict the sending 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 back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If the sending rate of ICMPv6 error messages is restricted due to excessive other ICMPv6 error messages, ICMPv6 Packet Too Big messages may be filtered, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages.

Although ICMPv6 Redirect packets are not ICMPv6 error messages, recommends restricting their rates together with ICMPv6 error messages except Packet Too Big messages.

Related Configuration

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval too-big** command to configure the sending rate of ICMPv6 Packet Too Big messages.

Configuring the Sending Rate of Other ICMPv6 Error Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval** command to configure the sending rate of other ICMPv6 error messages.

3.3.8 IPv6 Hop Limit

Working Principle

An IPv6 data packet passes through routers from the source address and 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 TTL of IPv4.

Related Configuration

Configuring the IPv6 Hop Limit

- The default IPv6 hop limit of a device is 64.
- Run the **ipv6 hop-limit** command to configure the IPv6 hop limit of a device.

3.3.9 Local ND Proxy

Working Principle

If the local ND proxy is enabled on an interface, the device can proxy its own MAC address to answer NA when it receives the NS request from a non-local host.

Related Configuration

↘ **Configuring Local ND Proxy**

- Run the **local-proxy-nd enable** command to enable local ND proxy in interface configuration mode.

3.4 Configuration

Configuration	Description and Command	
Configuring an IPv6 Address	⚠ (Mandatory) It is used to configure IPv6 addresses and enable IPv6.	
	ipv6 enable	Enables IPv6 on an interface.
	ipv6 address	Configures the IPv6 unicast address of an interface.
Configuring IPv6 NDP	⚠ (Optional) It is used to enable IPv6 redirection on an interface.	
	ipv6 redirects	Enables IPv6 redirection on an interface.
	⚠ (Optional) It is used to enable DAD.	
	ipv6 nd dad attempts	Configures the number of consecutive NS packets sent during DAD.
	⚠ (Optional) It is used to configure ND parameters.	
	ipv6 nd reachable-time	Configures the reachable time of a neighbor.
	ipv6 nd prefix	Configures the address prefix to be advertised in an RA packet.
	ipv6 nd suppress-ra	Enables RA suppression on an interface.
	⚠ (Optional) It is used to configure the maximum number of unresolved ND entries.	
	ipv6 nd unresolved	Configures the maximum number of unresolved ND entries.
	⚠ (Optional) It is used to configure the maximum number of neighbors learned on an interface.	
	ipv6 nd max-opt	Configures the maximum number of ND entries processed by the device.
	⚠ (Optional) It is used to configure the RDNSS options in the RA message.	
	ipv6 nd ra dns server	Configures RDNSS function and options.
	ipv6 nd cache interface-limit	Configures the maximum number of neighbors learned on an interface.
Configuring Path MTU Discovery	⚠ Optional. It is used to configure the maximum transmission unit of IPv6 packets.	
	ipv6 mtu	Sets the IPv6 MTU value.
Enabling IPv6 Source Routing	⚠ (Optional) It is used to enable IPv6 source routing.	
	ipv6 source-route	Configures the device to forward IPv6 packets carrying the routing header.
Configuring the Sending Rate of	⚠ Optional.	

Configuration	Description and Command	
ICMPv6 Error Messages	**ipv6 icmp error-interval too-big**	Configures the sending rate of ICMPv6 Packet Too Big messages.
	ipv6 icmp error-interval	Configures the sending rates of other ICMPv6 error messages and ICMPv6 Redirect packets.
Configuring the IPv6 Hop Limit	(Optional) It is used to restrict the hop limit of IPv6 unicast packets sent on an interface.	
	ipv6 hop-limit	Configures the IPv6 hop limit.
Configuring Local ND Proxy	(Optional) It is used to enable local ND proxy function on an interface.	
	local-proxy-nd enable	Enables local ND proxy on an interface.

3.4.1 Configuring an IPv6 Address

Configuration Effect

Configure the IPv6 address of an interface to implement IPv6 network communication.

Configuration Steps

Enabling IPv6 on an Interface

- (Optional) If you do not want to enable IPv6 by configuring an IPv6 address, run the **ipv6 enable** command.

Configuring the IPv6 Unicast Address of an Interface

- Mandatory.

Verification

Run the **show ipv6 interface** command to check whether the configured address takes effect.

Related Commands

Enabling IPv6 on an Interface

Command	**ipv6 enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IPv6 can be enabled on an interface by two methods: 1) running the **ipv6 enable** command in interface configuration mode; 2) configuring an IPv6 address on the interface. 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.

Configuring the IPv6 Unicast Address of an Interface

Command	**ipv6 address** *ipv6-address* / *prefix-length* **ipv6 address** *ipv6-prefix* / *prefix-length* **eui-64** **ipv6 address** *prefix-name sub-bits* / *prefix-length* [**eui-64**]
Param	*ipv6-address*: Indicates the IPv6 address, which must comply with the address format defined in

eter Description	RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits. *ipv6-prefix*: Indicates the IPv6 address prefix, which must comply with the address format defined in RFC 4291. *prefix-length*: Indicates the length of the IPv6 address prefix, that is, the part representing the network in the IPv6 address. *prefix-name*: Indicates the name of the universal prefix. This specified universal prefix is used to create the interface address. *sub-bits*: Indicates the subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* parameter. This value is combined with the universal prefix to create the interface address. This value must be in the form documented in RFC 4291. *eui-64*: Indicates the created IPv6 address, consisting of the configured address prefix and 64-bit interface ID.
Command Mode	Interface configuration mode
Usage Guide	If an IPv6 interface is created and is Up state, the system automatically generates a link-local address for this interface. The IPv6 address of an interface can also be created by the universal prefix mechanism. That is, IPv6 address = Universal prefix + Sub prefix + Host bits. The universal prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery function of the DHCPv6 client (see the *Configuring DHCPv6*). Sub prefix + Host bits are specified by the *sub-bits* and *prefix-length* parameters in the **ipv6 address** command. If you run the **no ipv6 address** command without specifying an address, all manually configured addresses will be deleted. Run the **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64** command to delete the configured address.

Configuration Example

↘ Configuring an IPv6 Address on an Interface

Configuration Steps	Enable IPv6 on the GigabitEthernet 0/0 interface and add IPv6 address 2000::1 to the interface.

	`Hostname(config)#interface gigabitEthernet 0/0`
	`Hostname(config-if-GigabitEthernet 0/0)#ipv6 enable`
	`Hostname(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64`

Verification	Run the **show ipv6 interface** command to verify that an address is successfully added to the GigabitEthernet 0/0 interface.

	`Hostname(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0`
	
	`interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0`
	`  address(es):`
	`    Mac Address: 00:00:00:00:00:00`
	`    INET6: FE80::200:FF:FE00:1 [ 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 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 200 seconds<160--240>

ND router advertisements live for 1800 seconds
```

Products do not support the VRF parameter. The above example is for reference purpose. Please take the actual device as standard.

3.4.2 Enabling PMTUD

Configuration Effect

When sending an IPv6 packet, a host fragments the packet based on the PMTU.

Notes

The IPv6 MTU of an interface must be less than or equal to the interface MTU.

Configuration Steps

Configuring the IPv6 MTU of an Interface

- Optional.

Verification

- Run the **show run** command to check whether the configuration is correct.
- Run the **show ipv6 interface** command to check whether the IPv6 MTU of an interface is correct.

Related Commands

Configuring the IPv6 MTU of an Interface

Command	**ipv6 mtu** *bytes*
Parameter Description	*bytes*: Indicates the MTU of an IPv6 packet, ranging from 1280 to 1500. The unit is byte.
Command Mode	Interface configuration mode

Usage Guide N/A

Configuration Example

Configuring the IPv6 MTU of an Interface

Configuration Steps Change the IPv6 MTU of interface GigabitEthernet 0/0 to 1,300.

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
```

Verification Run the **show ipv6 interface** command to check whether the configuration takes effect.

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface


interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:d0:f8:22:33:47
    INET6: FE80::2D0:F8FF:FE22:3347 [ TENTATIVE ], subnet is FE80::/64
    INET6: 1020::1 [ TENTATIVE ], subnet is 1020::/64
    INET6: 1023::1 [ TENTATIVE ], subnet is 1023::/64
  Joined group address(es):
  MTU is 1300 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 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 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
```

Common Errors

N/A

3.4.3 Configuring IPv6 NDP

Configuration Effect

Configure NDP-related attributes, for example, enable IPv6 redirection and DAD.

Notes

RA suppression is enabled on interfaces by default. To configure a device to send RA packets, run the **no ipv6 nd suppress-ra** command in interface configuration mode.

Configuration Steps

Enabling IPv6 Redirection on an Interface

- (Optional) IPv6 redirection is enabled by default.
- To disable IPv6 redirection on an interface, run the **no ipv6 redirects** command.

Configuring the Number of Consecutive NS Packets Sent During DAD

- Optional.
- To prevent enabling DAD for IPv6 addresses on an interface or modify the number of consecutive NS packets sent during DAD, run the **ipv6 nd dad attempts** command.

Configuring the Reachable Time of a Neighbor

- Optional.
- To modify the reachable time of a neighbor, run the **ipv6 nd reachable-time** command.

Enabling/Disabling RA Suppression on an Interface

- Optional.
- If a device needs to send RA packets, run the **no ipv6 nd suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

- Optional.
- If a large number of unresolved ND entries are generated due to scanning attacks, run the **ipv6 nd unresolved** command to restrict the number of unresolved neighbors.

Configuring the Maximum Number of ND Entries Learned on an Interface

- Optional.
- If the number of IPv6 hosts is controllable, run the **ipv6 nd cache interface-limit** command to restrict the number of neighbors learned on an interface. This prevents ND learning attacks from occupying the memory space and affecting device performance.

Verification

Run the following commands to check whether the configuration is correct:

- **show ipv6 interface** *interface-type interface-num*: Check whether the configurations such as the redirection function, reachable time of a neighbor, and NS sending interval take effect.
- **show ipv6 interface** *interface-type interface-num* **ra-inifo**: Check whether the prefix and other information configured for RA packets are correct.
- **show run**

Related Commands

Enabling IPv6 Redirection on an Interface

Command	**ipv6 redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All ICMPv6 error messages are transmitted at a limited transmission rate. By default, a maximum number of 10 ICMPv6 error messages are transmitted per second (10 pps).

Configuring the Number of Consecutive NS Packets Sent During DAD

Command	**ipv6 nd dad attempts** *value*
Parameter Description	*value*: Indicates the number of NS packets.
Command Mode	Interface configuration mode
Usage Guide	You need to enable DAD before configuring an IPv6 address on an interface. Then 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 uses EUI-64, 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 and restart the interface to re-enable DAD. When an interface changes from the down state to the up state, DAD is re-enabled for the addresses on this interface.

Configuring the Reachable Time of a Neighbor

Command	**ipv6 nd reachable-time** *milliseconds*
Parameter Description	*milliseconds*: Indicates the reachable time of a neighbor, ranging from 0 to 3,600,000. The unit is millisecond. The default value is 30s.
Command Mode	Interface configuration mode
Usage Guide	A device detects unreachable neighbors based on the configured reachable time. The shorter the configured reachable time, the faster the device detects unreachable neighbors but the more it consumes network bandwidth and device resources. Therefore, it is not recommended to set this time too small. The configured value is advertised in an RA packet and is also used on the device. If the value is 0, the reachable time is not specified on the device and it is recommended to use the default value.

Configuring the Address Prefix to Be Advertised in an RA Packet

Command	**ipv6 nd prefix {***ipv6-prefix/prefix-length* | **default**} [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite** {**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**] | [**preference** { high | medium | low }]]
Parameter Description	*ipv6-prefix*: Indicates the network ID of IPv6, which must comply with the address representation format in RFC 4291. *prefix-length*: Indicates the length of the IPv6 address prefix. A slash (/) must be added before the prefix.

	valid-lifetime: Indicates the period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 30 days. *preferred-lifetime*: Indicates the preferred period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 7 days. **at** *valid-date preferred-date*: Indicates the valid date and preferred deadline configured for the RA prefix. It uses the format of *dd+mm+yyyy+hh+mm*. **infinite**: Indicates that the prefix is permanently valid. **default**: Indicates that the default parameter configuration is used. **no-advertise**: Indicates that the prefix is not advertised by a router. **off-link**: If the prefix of the destination address in the IPv6 packet sent by a host matches the configured prefix, the device regards the destination address on the same link and directly reachable. This parameter indicates that this prefix does not require on-link determination. **no-autoconfig**: Indicates that the prefix in the RA packet received by a host cannot be used for address auto-configuration. **preference:** Sets the routing priority. The values are high, medium, and low.
Command Mode	Interface configuration mode
Usage Guide	This command can be used to configure parameters related to each prefix, including whether to advertise this prefix. By default, an RA packet uses the prefix configured by running the **ipv6 address** command. Run the **ipv6 nd prefix** command to add other prefixes. Run the **ipv6 nd prefix default** command to configure the default parameters for an interface. That is, if no parameter is specified when a prefix is added, use the parameters configured in the **ipv6 nd prefix default** command as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, when you use the **ipv6 nd prefix default** command to modify the default parameter configurations, only the prefix configured for the default parameters changes and configurations of the prefix remain the same. **at** *valid-date preferred-date*: You can specify the valid date of the prefix in two methods: 1) specifying a fixed time for each prefix in an RA packet; 2) specifying the deadline. In the second method, the valid date of the prefix in each RA packet decreases till it becomes 0.

Enabling/Disabling RA Suppression on an Interface

Command	**ipv6 nd suppress-ra**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To enable RA suppression on an interface, run the **ipv6 suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

Command	**ipv6 nd unresolved** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ND entries.
Command Mode	Global configuration mode
Usage Guide	To prevent malicious scanning attacks from creating a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

Configuring the Maximum Number of ND Entries Learned on an Interface

Command	**ipv6 nd cache interface-limit** *value*
Parameter Description	*value*: Indicates the maximum number of neighbors learned by an interface.
Command Mode	Interface configuration mode
Usage Guide	Restricting the number of ND entries learned on an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of ND entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the ND entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

Configuration Example

Enabling IPv6 Redirection on an Interface

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/0.
	`Hostname(config-if-GigabitEthernet 0/0)#ipv6 redirects`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.

	`Hostname#show ipv6 interface gigabitEthernet 0/0`
	
	`interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0`
	`  address(es):`
	`    Mac Address: 00:00:00:00:00:00`
	`    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/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 advertised reachable time is 0 milliseconds`
	`  ND retransmit interval is 1000 milliseconds`
	`  ND advertised retransmit interval is 0 milliseconds`

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/0.
	`Hostname(config-if-GigabitEthernet 0/0)#ipv6 redirects`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	`ND router advertisements are sent every 200 seconds<160--240>` `ND router advertisements live for 1800 seconds`

Configuring IPv6 DAD

Configuration Steps	Configure the interface to send three consecutive NS packets during DAD.
	`Hostname(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.

	`Hostname#show ipv6 interface gigabitEthernet 0/0`
	
	`interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0`
	`address(es):`
	`Mac Address: 00:00:00:00:00:00`
	`INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/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: 3`
	`ND reachable time is 30000 milliseconds`
	`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 200 seconds<160--240>`
	`ND router advertisements live for 1800 seconds`
	`Hostname(config-if-GigabitEthernet 0/0)#`
	Products do not support the VRF parameter. The above example is for reference purpose.

	Please take the actual device as standard.

Configuring Prefix Information in an RA Packet

Configuration Steps	Add a prefix 1234::/64 to interface GigabitEthernet 0/0.
	`Hostname(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.

	`Hostname#show ipv6 interface gigabitEthernet 0/0 ra-info`
	
	`GigabitEthernet 0/0: DOWN (RA is suppressed)`
	`  RA timer is stopped`
	`  waits: 0, initcount: 0`
	`  statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0`
	`  Link-layer address: 00:00:00:00:00:00`
	`  Physical MTU: 1500`
	`  ND router advertisements live for 1800 seconds`
	`  ND router advertisements are sent every 200 seconds<160--240>`
	`  Flags: !M!O, Adv MTU: 1500`
	`  ND advertised reachable time is 0 milliseconds`
	`  ND advertised retransmit time is 0 milliseconds`
	`  ND advertised CurHopLimit is 64`
	`  Prefixes: <total: 1>`
	`  1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)`

Configuring RA Packets to Obtain Prefixes from the Prefix Pool

Configuration Steps	Configure RA packets to obtain prefixes from the prefix pool "ra-pool".
	`Hostname(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Hostname(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0`

Configuration Steps	Configure RA packets to obtain prefixes from the prefix pool "ra-pool".
	`Hostname(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool`
Verification	Run the **show run** command to check whether the configuration takes effect.

	`Building configuration...`
	`Current configuration : 125 bytes`
	
	`interface GigabitEthernet 0/0`
	` ipv6 enable`
	` no ipv6 nd suppress-ra`
	`peel default ipv6 pool ra-pool`
	`!`

Disabling RA Suppression

Configuration Steps	Disable RA suppression on an interface.
	`Hostname(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra`
Verification	Run the **show run** command to check whether the configuration takes effect.

	`Hostname(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0`
	
	`Building configuration...`
	`Current configuration : 125 bytes`
	
	`interface GigabitEthernet 0/0`
	` ipv6 enable`
	` no ipv6 nd suppress-ra`
	`!`

Configuring the Maximum Number of Unresolved ND Entries

Configuration Steps	Set the maximum number of unresolved ND entries to 200.

	Hostname(config)# ipv6 nd unresolved 200
Verification	Run the **show run** command to check whether the configuration takes effect.
	Hostname#show run ipv6 nd unresolved 200 !

Configuring the Maximum Number of ND Entries Learned on an Interface

Configuration Steps	Set the maximum number of ND entries learned on an interface to 100.
	Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
Verification	Run the **show run** command to check whether the configuration takes effect.
	Hostname#show run ! interface GigabitEthernet 0/1 ipv6 nd cache interface-limit 100 !

3.4.4 Enabling IPv6 Source Routing

Configuration Effect

RFC 5095 abolished the Type 0 routing header. This series does not support the Type 0 routing header by default. The administrator can run the **ipv6 source-route** command to in global configuration mode to enable IPv6 source routing.

Configuration Steps

Enabling IPv6 Source Routing

- Optional.
- To enable IPv6 source routing, run the **ipv6 source-route** command.

Verification

The device can properly forward packets carrying the Type 0 routing header.

Related Commands

Enabling IPv6 Source Routing

Command	**ipv6 source-route**

and	
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Since the Type 0 header may cause the device prone to DoS attacks, the device does not forward IPv6 packets carrying the routing header by default, but still processes IPv6 packets with itself being the final destination address and the Type 0 routing header.

Configuration Example

Enabling IPv6 Source Routing

Configuration Steps	Enable IPv6 source routing.
	`Hostname(config)#ipv6 source-route`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Hostname#show run | inc ipv6 source-route` `ipv6 source-route`

3.4.5 Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Effect

Configure the sending rate of ICMPv6 error messages.

Configuration Steps

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- Optional.
- If a device receives many IPv6 packets with the packet length exceeding the IPv6 MTU of the outbound interface and thereby sends many ICMPv6 Packet Too Big messages to consume much CPU resources, run the **ipv6 icmp error-interval too-big** command to restrict the sending rate of this error message.

Configuring the Sending Rate of Other ICMPv6 Error Messages

- Optional.
- If a device receives many illegal IPv6 packets and thereby generates many ICMPv6 error messages, run the **ipv6 icmp error-interval** command to restrict the sending rate of ICMPv6 error messages. (This command does not affect the sending rate of ICMPv6 Packet Too Big messages.)

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Command	**ipv6 icmp error-interval too-big** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending 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 back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If other ICMPv6 error messages are excessive, ICMPv6 Packet Too Big messages cannot be sent, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Command	**ipv6 icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuration Example

Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Steps	Set the sending rate of the ICMPv6 Packet Too Big message to 100 pps and that of other ICMPv6 error messages to 10 pps.

	Hostname(config)#ipv6 icmp error-interval too-big 1000 100 Hostname(config)#ipv6 icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Hostname#show running-config | include ipv6 icmp error-interval ipv6 icmp error-interval 1000 10 ipv6 icmp error-interval too-big 1000 100

3.4.6 Configuring the IPv6 Hop Limit

Configuration Effect

Configure the number of hops of a unicast packet to prevent the packet from being unlimitedly transmitted.

Configuration Steps

Configuring the IPv6 Hop Limit

- Optional.
- To modify the number of hops of a unicast packet, run the **ipv6 hop-limit value** command.

Verification

- Run the **show running-config** command to check whether the configuration is correct.
- Capture the IPv6 unicast packets sent by a host. The packet capture result shows that the hop-limit field value in the IPv6 header is the same as the configured hop limit.

Related Commands

Configuring the IPv6 Hop Limit

Command	**ipv6 hop-limit value**
Parameter Description	*value*: Indicates the number of hops of a unicast packet sent by the device. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the IPv6 Hop Limit

Configuration Steps	Change the IPv6 hop limit of a device to 250.
	Hostname(config)#ipv6 hop-limit 250

Verification	Run the **show running-config** command to check whether the configuration takes effect.
	`Hostname#show running-config` `ipv6 hop-limit 254`

3.4.7 Configuring Local ND Proxy

Configuration Effect

Enable local ND proxy on an interface.

Notes

N/A

Configuration Steps

Configuring local ND proxy function on the device (usually the gateway)

- Optional.
- Run this command to enable local ND proxy on an interface when necessary.

Verification

After configuration, if the gateway receives the NS request message, but the destination IP address of the request is not the gateway interface's IP address (but on the same segment), the MAC of the proxy gateway responds with NA.

Related Commands

Configuring the device to forward IPv6 packets with routing header

Command	**local-proxy-nd enable**
Parameter Description	N/A
Command Mode	Layer 3 interface configuration mode
Usage Guide	When the access is two-layer isolation or isolation between different subnets (such as subvlans), the gateway will proxy the NS requests of the downlink users and answer with its own MAC if the local ND proxy function is enabled on the gateway, so that the mutual access traffic between users can be forwarded over Layer 3 of the gateway.

Configuration Example

Configuring the interface to support local ND proxy.

Configuration Steps Enable local ND proxy on the VLAN1 interface.

```
Ruijie(config-if- VLAN 1)# local-proxy-nd enable
```

Verification Run the **show running-config** command to check whether the configuration takes effect.

```
Ruijie#show run interface vlan 1

local-proxy-nd enable
```

Common Errors

N/A

3.5 Monitoring

Clearing

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

Description	Command
Clears the dynamically learned neighbors.	**clrear ipv6 neighbors** [*interface-id*]

Displaying

Description	Command
Displays IPv6 information of an interface.	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
Displays neighbor information.	**show ipv6 neighbors** [**verbose**] [*interface-id*] [*ipv6-address*] [static]

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ND entry learning.	**debug ipv6 nd**

4 Configuring DHCP

4.1 Overview

The Dynamic Host Configuration Protocol (DHCP) is a LAN protocol based on the User Datagram Protocol (UDP) for dynamically assigning reusable network resources, 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 a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC3046: DHCP Relay Agent Information Option

4.2 Applications

Application	Description
Providing DHCP Service in a LAN	Assigns IP addresses to clients in a LAN.
Enabling DHCP Client	Enable DHCP Client.
Deploying DHCP Relay in Wired Network	In a wired network, users from different network segments requests IP addresses.

4.2.1 Providing DHCP Service in a LAN

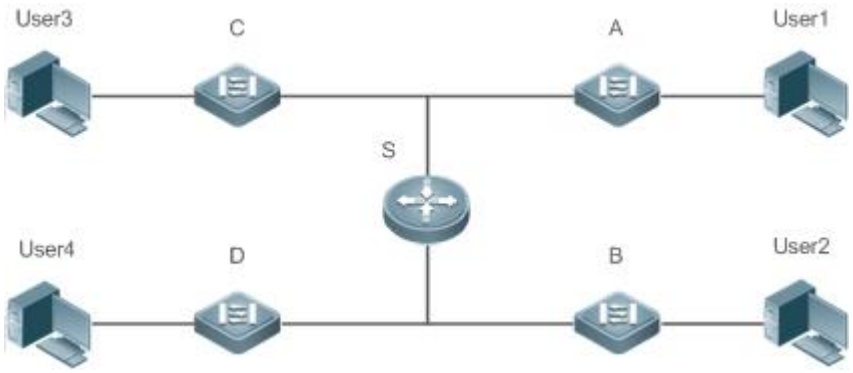
Scenario

Assign IP addresses to four users in a LAN.

For example, assign IP addresses to User 1, User 2, User 3 and User 4, as shown in the following figure.

- The four users are connected to Server S through A, B, C and D.

Figure 4-1



Remarks	S is an egress gateway working as a DHCP server. A, B, C and D are access switches achieving layer-2 transparent transmission. User 1, User 2, User 3 and User 4 are LAN users.

Deployment

- Enable DHCP Server on S.
- Deploy layer-2 VLAN transparent transmission on A, B, C and D.
- User 1, User 2, User 3 and User 4 initiate DHCP client requests.

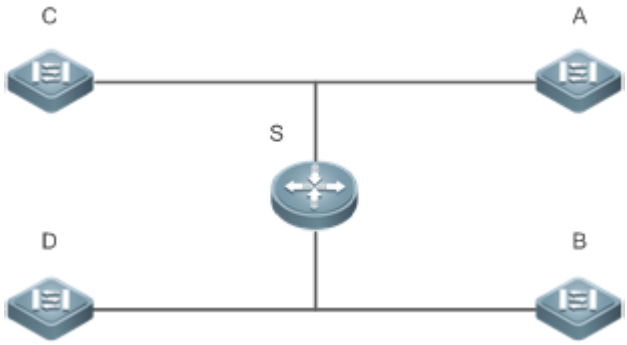
4.2.2 Enabling DHCP Client

Scenario

Access switches A, B, C and D in a LAN request server S to assign IP addresses.

For example, enable DHCP Client on the interfaces of A, B, C and D to request IP addresses, as shown in the following figure.

Figure 4-2



Remarks	S is an egress gateway working as a DHCP server. A, B, C and D are access switches with DHCP Client enabled on the interfaces.

Deployment

- Enable DHCP Server on S.
- Enable DHCP Client on the interfaces of A, B, C and D.

4.2.3 Deploying DHCP Relay in Wired Network

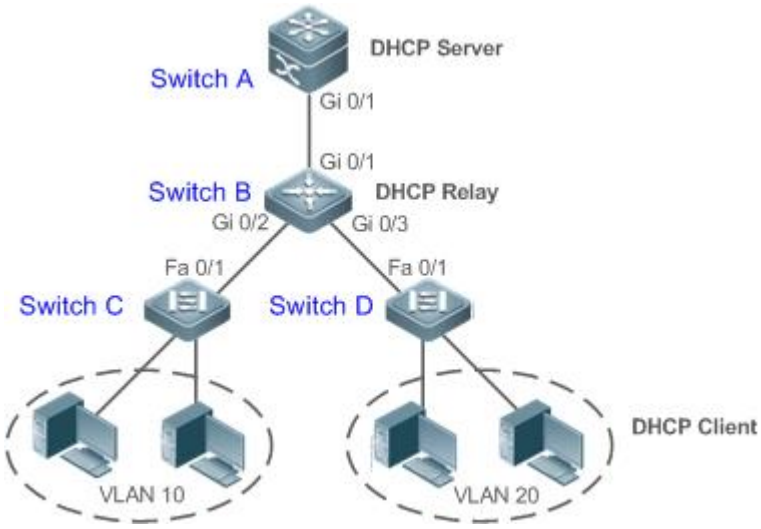
Scenario

As shown in the following figure, Switch C and Switch D are access devices for the users in VLAN 10 and VLAN 20 respectively. Switch B is a gateway, and Switch A a core device. The requirements are listed as follows:

Switch A works as a DHCP server to assign IP addresses of different network segments dynamically to users in different VLANs.

Users in VLAN 10 and VLAN 20 obtain IP addresses dynamically.

Figure 4-3 DHCP Relay



Remarks	Switch C and Switch D are access devices. Switch B is a gateway. Switch A is a core device.

Deployment

- Configure layer-2 communication between Switch B and Switch C as well as between Switch B and Switch D.
- On Switch B, specify a DHCP server address and enable DHCP Relay.
- On Switch A, create DHCP address pools for VLAN 10 and VLAN 20 respectively, and enable DHCP Server.

4.2.4 Typical Application of Out-of-the-Box Manageable Features

Scenario

If the device does not have a serial port, and the administrator wants to access the device through the web management system or telnet, a boot management IP address must be dynamically assigned to the device. After the device obtains the dynamic IP address, since the administrator does not know the dynamically obtained IP address, so the boot management IP address must be configured as a second IP address after the device obtains a dynamic IP address.

Deployment

If the device is booted without the config.text configuration file, the device is considered to have booted out of box.

4.3 Features

Basic Concepts

DHCP Server

Based on the RFC 2131, our DHCP server assigns IP addresses to clients and manages these IP addresses.

DHCP Client

DHCP Client enables a device to automatically obtain an IP address and configurations from a DHCP server.

DHCP Relay

When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Lease

Lease is a period of time specified by a DHCP server for a client to use an assigned IP address. An IP address is active when leased to a client. 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 becomes inactive.

Excluded Address

An excluded address is a specified IP address not assigned to a client by a DHCP server.

Address Pool

An address pool is a collection of IP addresses that a DHCP server may assign to clients.

Option Type

An option type is a parameter specified by a DHCP server when it provides lease service to a DHCP client. For example, a public option include the IP addresses of a default gateway (router), WINS server and a DNS server. DHCP server allows configuration of other options. Though most options are defined in the RFC 2132, you can add user-defined options.

Overview

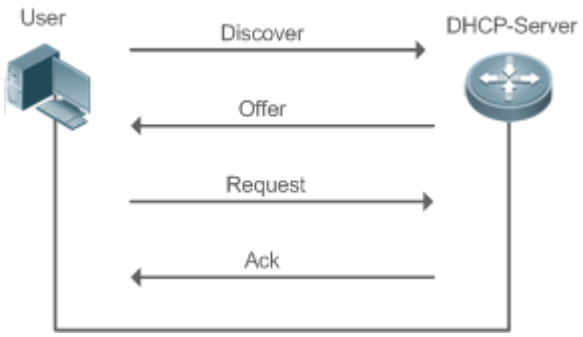
Feature	Description
DHCP Server	Enable DHCP Server on a device, and it may assign IP addresses dynamically and pushes configurations to DHCP clients.
DHCP Relay Agent	Enable DHCP Relay on a device, and it may forward DHCP request and reply packets across different network segments.
DHCP Client	Enable DHCP Client on a device, and it may obtain IP addresses and configurations automatically from a DHCP server.

4.3.1 DHCP Server

Working Principle

DHCP Working Principle

Figure 4-4



A host requests an IP address through DHCP as follows:

1. A host broadcasts a DHCP discover packet to find DHCP servers in a network.
2. DHCP servers unicast/broadcast (based on the property of the host packet) DHCP offer packets to the host, containing an IP address, a MAC address, a domain name and a lease.
3. The host broadcasts a DHCP request packet to formally request an IP address.
4. A DHCP server sends a DHCP ACK unitcast packet to the host to acknowledge the request.

A DHCP client may receive DHCPOFFER packets from multiple DHCP servers, but usually it accepts only the first DHCPOFFER packet. Besides, the address specified in a DHCPOFFER packet is not necessarily assigned. Instead, it is retained by the DHCP server until a client sends a formal request.

To formally request an IP address, a client broadcasts a DHCPREQUEST packet so that all DHCP servers sending DHCPOFFER packets may receive the packet and release OFFER IP addresses.

If a DHCPOFFER packet contains invalid configuration parameters, a client will send a DHCPDECLINE packet to the server to decline the configuration.

During the negotiation, if a client does not respond to the DHCPOFFER packets in time, servers will send DHCPNAK packets to the client and the client will reinitiate the process.

During network construction, our DHCP servers have the following features:

- Low cost. Usually the static IP address configuration costs more than DHCP configuration.
- Simplified configuration. Dynamic IP address assignment dramatically simplifies device configuration
- Centralized management. You can modify the configuration for multiple subnets by simply modifying the DHCP server configuration.

Address Pool

After a server receives a client's request packet, it chooses a valid address pool, determines an available IP address from the pool through PING, and pushes the pool and address configuration to the client. The lease information is saved locally for validity check upon lease renewal.

An address pool may carry various configuration parameters as follows:

- An IP address range, which is the range of IP addresses that are available.
- A gateway address. A maximum of 8 gateway addresses are supported.
- A DNS address. A maximum of 8 DNS addresses are supported.
- A lease period notifying clients of when to age an address and request a lease renewal.

VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, devices enabled with DHCP provide a command to monitor the VRRP status of the interface. To an interface configured with VRRP address and VRRP monitoring, a DHCP server only processes the DHCP clients' request packets from the interface in Master state, and other packets are discarded. If no VRRP address is configured, the DHCP server does not monitor the VRRP status, and all DHCP packets are processed. VRRP monitoring is configured on only layer-3 interfaces. It is disabled by default, namely, only the Master device processes the DHCP service.

ARP-Based Offline Detection

Devices enabled with DHCP provide a command to enable ARP-based offline detection. After this function is enabled, a DHCP server will receive an ARP aging notification when a client gets offline, and start retrieving the client's address. If the client does not get online within a period of time (5 minutes by default), the DHCP server will retrieve the address and assign it to another client. If the client gets online again, the address is still valid.

Adding Pseudo Server Detection

If a DHCP server is deployed illegally, a client interacts with this server while requesting an IP address and a wrong address will be assigned to the client. This server is a pseudo server. Devices enabled with DHCP provides a command to enable pseudo server detection. After it is enabled, DHCP packets are checked for Option 54 (Server Identifier Option). If the content of Option 54 is different from the actual DHCP server identifier, the IP address of the pseudo server and port receiving the packets will be recorded. The pseudo server detection is only an after-event security function and cannot prevent an illegal DHCP server from assigning IP addresses to clients.

Related Configuration

Enabling DHCP Server Globally

- By default, DHCP Server is disabled.
- Run the **service dhcp** command to enable the DHCP Server.
- Run the **service dhcp** command globally to enable DHCP service.

Configuring Address Pool

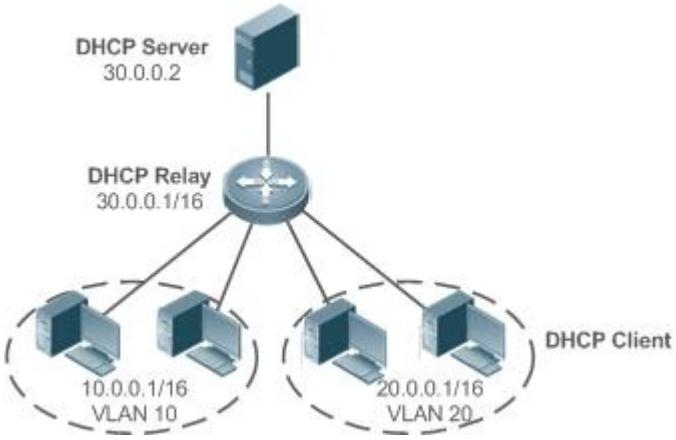
- By default, no address pool is configured.
- Run the **ip dhcp pool** command to configure an IP address range, a gateway and a DNS.
- If no address pool is configured, no addresses will be assigned.

4.3.2 DHCP Relay Agent

Working Principle

The destination IP address of DHCP request packets is 255.255.255.255, and these packets are forwarded within a subnet. To achieve IP address assignment across network segments, a DHCP relay agent is needed. The DHCP relay agent unicasts DHCP request packets to a DHCP server and forwards DHCP reply packets to a DCHP client. The DHCP relay agent serves as a repeater connecting a DHCP client and a DHCP server of different network segments by forwarding DHCP request packets and DHCP reply packets. The Client-Relay-Server mode achieves management of IP addresses across multiple network segments by only one DHCP server. See the following figure.

Figure 4-5 DHCP Relay Scenario



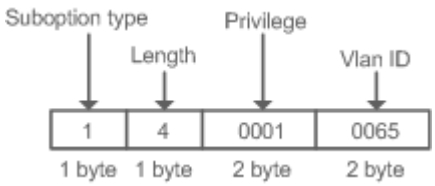
VLAN 10 and VLAN 20 correspond to the segments 10.0.0.1/16 and 20.0.0.1/16 respectively. A DHCP server with IP address 30.0.0.2 is in segment 30.0.0.1/16. To achieve management of dynamic IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable DHCP Relay on a gateway and configure IP address 30.0.0.2 for the DHCP server.

DHCP Relay Agent Information (Option 82)

As defined in RFC3046, an option can be added to indicate a DHCP client's network information when DHCP Relay is performed, so that a DHCP server may assign IP addresses of various privileges based on more accurate information. The option is called Option 82. Currently, devices support four schemes of relay agent information, which are described respectively as follows:

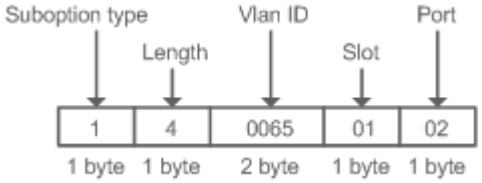
Relay agent information option dot1x: This scheme should be implemented with 802.1X authentication and the RG-SAM products. Specifically, RG-SAM products push the IP privilege during 802.1X authentication. A DHCP relay agent forms a Circuit ID sub-option based on the IP privilege and the VLAN ID of a DHCP client. The option format is shown in the following figure.

Figure 4-6 Option Format



Relay agent information option82: This scheme serves without correlation with other protocol modules. A DHCP relay agent forms an Option 82 based on the physical port receiving DHCP request packets and the MAC address of the device. The option format is shown in the following figure.

Figure 4-7 Agent Circuit ID



Relay agent information option82: This scheme serves without correlation with other protocol modules. Compared with previous Option 82, this option supports user-defined content, which may change. By default, a DHCP relay agent forms Option 82 according to the information of the physical port receiving DHCP packets, device MAC address and device name. The option format is shown in the following figure.

Figure 4-8 Option82.1-circuit-id

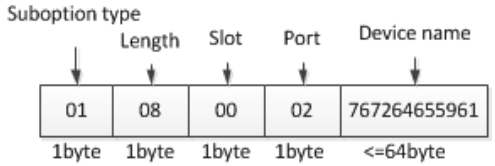
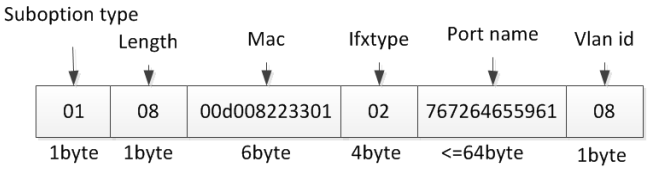


Figure 4-9 Option82-remote-id



DHCP Relay Check Server-ID

In DHCP environment, multiple DHCP servers are deployed for a network, achieving server backup to ensure uninterrupted network operation. After this function is enabled, the DHCP request packet sent by a client contains a **server-id** option specifying a DHCP server. In alleviating the burden on servers in specific environments, you need to enable this function on a relay agent to send a packet to a specified DHCP server rather than all DHCP servers.

DHCP Relay suppression

After you configure the **ip dhcp relay suppression** command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP request packets will be forwarded.

Related Configuration

Enabling DHCP Relay

- By default, DHCP Relay is disabled.
- You may run the **service dhcp** command to enable DHCP Relay.
- You need to enable DHCP Relay before it works.

Configuring IP Address for DHCP Server

- By default, no IP address is configured for a DHCP server.
- You may run the **ip helper-address** command to configure an IP address for a DHCP server. The IP address can be configured globally or on a layer-3 interface. A maximum of 20 IP addresses can be configured for a DHCP server.
- When an interface receives a DHCP request packet, the DHCP server configuration on the interface prevails over that configured globally. If the interface is not configured with DHCP server addresses, the global configuration takes effect.

Enabling DHCP Option 82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable DHCP Option 82.

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Enabling DHCP Relay Suppression

- By default, DHCP Relay suppression is disabled on all interfaces.
- You may run the **ip dhcp relay suppression** command to enable it on an interface.

4.3.3 DHCP Client

Working Principle

A DHCP client broadcasts a DHCP discover packet after entering the Init state. Then it may receive multiple DHCP offer packets. It chooses one of them and responds to the corresponding DHCP server. After that, it sends lease renewal request packets in the Renew and Rebind processes of an aging period to request lease renewal.

Related Configuration

Enabling DHCP Client on Interface

- By default, DHCP Client is disabled.
- In interface configuration mode, you may run the **ip address dhcp** command to enable DHCP Client.
- You need to enable DHCP Client to enable DHCP service.
- The configuration takes effect on a layer-3 interface, for example, an SVI or a routed port.

4.4 Configuration

Configuring DHCP Server

Configuration	Description and Command	
Configuring Dynamic IP Address	⚠ (Mandatory) It is used to enable DHCP Server to achieve dynamic IP address assignment.	
	service dhcp	Enables DHCP Server.
	ip dhcp pool	Configures an address pool.
	network	Configures the network number and subnet mask of a DHCP address pool.

Configuration	Description and Command	
	(Optional) It is used to configure the properties of an address pool.	
	default-router	Configures a default gateway of a client.
	lease	Configures an address lease.
	next-server	Configures a TFTP server address
	bootfile	Configures a boot file of a client.
	domain-name	Configures a domain name of a client.
	dns-server	Configures a domain name server.
	netbios-name-server	Configures a NetBIOS WINS server.
	netbios-node-type	Configures a NetBIOS node type on a client.
	lease-threshold	Configures an alarm threshold of an address pool.
	option	Configures a user-defined option.
	pool-status	Enables or disables an address pool.
Configuring Static IP Address	(Optional) It is used to statically assign an IP address to a client.	
	ip dhcp pool	Configures an address pool name and enters address pool configuration mode.
	host	Configures the IP address and subnet mask of a client host.
	hardware-address	Configures a client hardware address.
	client-identifier	Configures a unique client identifier.
	client-name	Configures a client name.
Configuring Global Properties of DHCP Server	(Optional) It is used to configure the properties of a DHCP server.	
	ip dhcp excluded-address	Configures an excluded IP address.
	ip dhcp force-send-nak	Configures Compulsory NAK reply by a DHCP server.
	ip dhcp monitor-vrrp-state	Configures VRRP status monitoring.
	ip dhcp ping packets	Configures ping times.
	ip dhcp ping timeout	Configures a ping timeout.
	ip dhcp server arp-detect	Configures a DHCP server to detect user offline.

Configuring DHCP Relay

Configuration	Description and Command	
Configuring Basic DHCP Relay Functions	(Mandatory) It is used to enable DHCP Relay.	
	service dhcp	Enables DHCP Relay.
	ip helper-address	Configures an IP Address of a DHCP Server.

Configuration	Description and Command	
Configuring DHCP Relay Option 82	(Optional) It is used to assign IP addresses of different privileges to clients in combination with the information of a physical port. This function cannot be used together with the **dhcp option dot1x** command.	
	ip dhcp relay information option82	Enables DHCP option82.
Configuring DHCP Relay Check Server-ID	(Optional) It is used to enable a DHCP Relay agent to send DHCP request packets only to a specified server.	
	ip dhcp relay check server-id	Enables a DHCP Relay agent to send DHCP request packets only to a specified server
Configuring DHCP Relay Suppression	(Optional) It is used to shield DHCP request packets on an interface.	
	ip dhcp relay suppression	Enables DHCP Relay Suppression.

Configuring DHCP Client

Configuration	Description and Command	
Configuring DHCP Client	(Mandatory) It is used to enable DHCP Client.	
	ip address dhcp	Enables an Ethernet interface, a PPP/HDLC-encapsulated or FR-encapsulated interface to obtain IP addresses through DHCP.

4.4.1 Configuring Dynamic IP Address

Configuration Effect

Provide all DHCP clients with DHCP service including assigning IP addresses and gateways.

Notes

A DHCP server and a DHCP relay share the **service dhcp** command, but 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 and forwards packets. Otherwise, it serves as a relay agent.

Configuration Steps

Enabling DHCP Server

- Mandatory. It achieves dynamic IP address assignment.
- Run the **service dhcp** command in global configuration mode.

Configuring Address Pool

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

- Mandatory. It defines a range of dynamically assigned addresses.
- Run the **network** command in DHCP address pool configuration mode.

Configuring Default Gateway of Client

- Optional. It is used to configure a gateway address.
- Run the **default-router** command in DHCP address pool configuration mode.

Configuring Address Lease

- Optional. It is used to configure an IP address lease, which is 24h by default.
- Run the **lease** command in DHCP address pool configuration mode.

Configuring TFTP Server Address

- Optional. It is used to configure a TFTP server address.
- Run the **next-server** command in DHCP address pool configuration mode.

Configuring Domain Name of Client

- Optional. It is used to configure the domain name of a client.
- Run the **domain-name** command in DHCP address pool configuration mode.

Configuring DNS

- Optional. It is used to configure a DNS address.
- Run the **dns** command in DHCP address pool configuration mode.

Configuring NetBIOS WINS Server

- Optional. It is used to configure a NetBIOS WINS server address.
- Run the **netbios-name-server** command in DHCP address pool configuration mode.

Configuring NetBIOS Node Type on Client

- Optional. It is used to configure a NetBIOS node type.
- Run the **netbios-name-type** command in DHCP address pool configuration mode.

Configuring Alarm Threshold of Address Pool

- Optional. It is used to manage the number of leases. When a threshold (90% by default) is reached, an alarm will be printed.
- Run the **lease-threshold** command in DHCP address pool configuration mode.

Configuring User-Defined Option

- Optional. It is used to configure user-defined options.
- Run the **option** command in DHCP address pool configuration mode.

Enabling or Disabling Address Pool

- Optional. It is used to enable or disable an address pool. It is enabled by default.
- Run the **pool-status** command in DHCP address pool configuration mode.

Verification

Connect a DHCP client and a DHCP server.

- Check whether the client obtains configurations on the server.

Related Commands

Enabling DHCP Server

Command	**service dhcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable DHCP Server and DHCP Relay. A DHCP server and a DHCP relay share the **service dhcp** command. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter DHCP address pool configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

Command	**network** *network-number mask* [*low-ip-address high-ip-address*]
Parameter Description	*network-number:* Indicates the network number of an IP address pool. *mask:* Indicates the subnet mask of an IP address pool. If no subnet mask is defined, the natural subnet mask is applied.
Command Mode	DHCP address pool configuration mode
Usage Guide	To configure dynamic address assignment, you need to configure a network number and subnet mask of an address pool to provide a DHCP server with a range of addresses. The IP addresses in a pool are assigned in order. If an address is assigned or exists in the target network segment, the next address will be checked until a valid address is assigned. For our products, addresses are assigned based on the client's physical address and ID. Therefore, one client will not be assigned two leases from one address pool. In case of topological redundancy between a client and a server, address assignment may fail. To avoid such failures, a network administrator needs to prevent path redundancy in network construction, for example, by adjusting physical links or network paths.

Configuring Default Gateway of Client

Comm	**default-router** *address* [*address2…address8*]

and	
Parameter Description	*address*: Indicates the IP address of a default gateway. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 gateways can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure a default gateway of a client, and a server will push the gateway configuration to the client. The IP addresses of the default gateway and the client should be in a same network.

Configuring Address Lease

Command	**lease** {*days* [*hours]* [*minutes*]	**infinite**}
Parameter Description	*days:* Defines a lease in the unit of day. *hours:* (Optional) Defines a lease in the unit of hour. Please define *days* before *hours*. *minutes:* (Optional) Defines a lease in the unit of minute. Please define *days* and *hours* before *minutes*. **infinite:** Defines an unlimited lease.
Command Mode	DHCP address pool configuration mode
Usage Guide	The default lease of an IP address assigned by a DHCP server is 1 day. When a lease is expiring soon, a client needs to request a lease renewal. Otherwise the IP address cannot be used after the lease is expired.

Configures Boot File on Client

Command	**bootfile** *filename*
Parameter Description	*file-name*: Defines a boot file name.
Command Mode	DHCP address pool configuration mode
Usage Guide	A boot file is a bootable image file used when a client starts up. The file is usually an OS downloaded by a DHCP client.

Configuring Domain Name of Client

Command	**domain-name** *domain*
Parameter Description	*domain-name:* Defines a domain name of a DHCP client.
Command Mode	DHCP address pool configuration mode
Usage Guide	You may define a domain name for a client. When the client accesses network through the host name, the domain name will be added automatically to complete the host name.

Configuring DNS

Command	**dns-server** { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }
Parameter Description	*ip-address:* Defines an IP address of a DNS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 DNS servers can be configured. **use-dhcp-client** *interface-type interface-number:* A DHCP client learns its DNS server via system software.
Command Mode	DHCP address pool configuration mode
Usage Guide	If a client accesses network resources through the domain name, you need to configure a DNS server to resolve the domain name.

Configuring NetBIOS WINS Server

Command	**netbios-name-server** *address* [*address2…address8*]
Parameter Description	*address:* Defines an IP address of a WINS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 WINS servers can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	WINS is a domain name service through which a Microsoft TCP/IP network resolves a NetNBIOS name to an IP address. A WINS server is a Windows NT server. When a WINS server starts, it receives a registration request from a WINS client. When the client shuts down, it sends a name release message, so that the computers in the WINS database and on the network are consistent.

Configuring NetBIOS Node Type on Client

Command	**netbios-node-type** *type*
Parameter Description	type: Defines a NetBIOS node type with one of the following approaches. 1. A hexadecimal number, ranging from 0 to FF. Only followings values are available. ● b-node ● p-node ● m-node ● 8 for h-node 2. A character string. ● b-node for a broadcast node; ● p-node for a peer-to-peer node; ● m-node for a mixed node; ● h-node for a hybrid mode.
Command Mode	DHCP address pool configuration mode
Usage Guide	There are four types of NetBIOS nodes of a Microsoft DHCP client. (1) A broadcast node. For such a node, NetBIOS name resolution is requested through broadcast. (2) A peer-to-peer node. The client sends a resolution request to the WINS server. (3) A mixed node. The client broadcasts a resolution request and sends the resolution request to the WINS server. (4) A hybrid node. The client sends a resolution request to the WINS server. If no reply is received, the client will broadcast the resolution request. By default, a Microsoft operating system is a broadcast or hybrid node. If no WINS server is configured, it is a broadcast node. Otherwise, it is a hybrid node.

Configuring User-Defined Option

Comm	**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

and	
Parameter Description	*code:* Defines a DHCP option code. **ascii** *string:* Defines an ASCII character string. **hex** *string:* Defines a hexadecimal character string. **ip** *ip-address:* Defines an IP address.
Command Mode	DHCP address pool configuration mode
Usage Guide	The DHCP allows transmitting configuration information to a host via a TCP/IP network. DHCP packets contain the option field of definable content. A DHCP client should be able to receive a DHCP packet carrying at least 312 bytes option. Besides, the fixed data field in a DHCP packet is also called an option.

Enabling or Disabling Address Pool

Command	**pool-status** {**enable	disable**}
Parameter Description	**enable***:* Enables an address pool. **disable***:* Disable an address pool. It is enabled by default.
Command Mode	DHCP address pool configuration mode
Usage Guide	N/A

Configuration Example

Configuring Address Pool

Configuration Steps	• Define an address pool net172. • The network segment is 172.16.1.0/24. • The default gateway is 172.16.1.254. • The address lease is 1 day. • xcluded addresses range from 172.16.1.2 to 172.16.1.100.
	Hostname(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100 Hostname(dhcp-config)# ip dhcp pool net172 Hostname(dhcp-config)# network 172.16.1.0 255.255.255.0 Hostname(dhcp-config)# default-router 172.16.1.254 Hostname(dhcp-config)# lease 1
Verification	Run the **show run** command to display the configuration.
	Hostname(config)#show run	begin ip dhcp ip dhcp excluded-address 172.16.1.2 172.16.1.100 ip dhcp pool net172 network 172.16.1.0 255.255.255.0default-router 172.16.1.254

	lease 1

4.4.2 Configuring Static IP Address

Configuration Effect

Assign specific IP addresses and push configuration to specific DHCP clients.

Notes

N/A

Configuration Steps

Configuring Address Pool Name and Entering Address Pool Configuration Mode

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring IP Address and Subnet Mask of Client

- Mandatory. It is used to configure a static IP address and a subnet mask.
- Run the **host** command in DHCP address pool configuration mode.

Configuring Hardware Address of Client

- Optional. It is used to configure a MAC address.
- Run the **hardware** command in DHCP address pool configuration mode.

Configures Unique Client Identifier

- Optional. It is used to configure a static user identifier (UID).
- Run the **client-identifier** command in DHCP address pool configuration mode.

Configuring Client Name

- Optional. It is used to configure a static client name.
- Run the **host-name** command in DHCP address pool configuration mode.

Verification

Check whether the client obtains the IP address when it is online.

Related Commands

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter address pool configuration mode.

Manual IP Address Binding

Command	**host** *ip-address* [*netmask*] **client-identifier** *unique-identifier* **client-name** *name*
Parameter Description	*ip-address:* Defines the IP address of a DHCP client. *netmask:* Defines the subnet mask of a DHCP client. *unique-identifier:* Defines the hardware address (for example, aabb.bbbb.bb88) and identifier (for example, 01aa.bbbb.bbbb.88) of a DHCP client. *name:* (Optional) It defines a client name using ASCII characters. The name excludes a domain name. For example, name a host **mary** rather than **mary.rg.com**.
Command Mode	DHCP address pool configuration mode
Usage Guide	Address binding means mapping between an IP address and a client's MAC address. There are two kind of address binding. 1) Manual binding. Manual binding can be deemed as a special DHCP address pool with only one address. 2) Dynamic binding. A DHCP server dynamically assigns an IP address from a pool to a client when it receives a DHCP request, creating mapping between the IP address and the client's MAC address. To configure manual binding, you need to define a host pool and then specify a DHCP client's IP address and hardware address or identifier. A hardware address is a MAC address. A client identifier includes a network medium type and a MAC address. A Microsoft client is usually identified by a client identifier rather than a MAC address. For the codes of medium types, refer to the *Address Resolution Protocol Parameters* section in the RFC 1700. The Ethernet type is **01**.

Configuration Example

Dynamic IP Address Pool

Configuration Steps	● Configure address pool VLAN 1 with IP address 20.1.1.0 and subnet mask 255.255.255.0. ● The default gateway is 20.1.1.1. ● The lease time is 1 day.
	Hostname(config)# ip dhcp pool vlan1 Hostname(dhcp-config)# network 20.1.1.0 255.255.255.0 Hostname(dhcp-config)# default-router 20.1.1.1 Hostname(dhcp-config)# lease 1 0 0
Verification	● Run the **show run** command to display the configuration.
	Hostname(config)#show run | begin ip dhcp ip dhcp pool vlan1 network 20.1.1.0 255.255.255.0 default-router 20.1.1.1 lease 1 0 0

Manual Binding

Configuration	● The host address is 172.16.1.101 and the subnet mask is 255.255.255.0. ● The host name is Billy.rg.com. ● The default gateway is 172.16.1.254.

Steps	● The MAC address is 00d0.df34.32a3.
	Hostname(config)# ip dhcp pool Billy Hostname(dhcp-config)# host 172.16.1.101 255.255.255.0 Hostname(dhcp-config)# client-name Billy Hostname(dhcp-config)# hardware-address 00d0.df34.32a3 Ethernet Hostname(dhcp-config)# default-router 172.16.1.254
Verification	Run the **show run** command to display the configuration.
	Hostname(config)#show run | begin ip dhcp ip dhcp pool Billy host 172.16.1.101 255.255.255.0 client-name Billy hardware-address 00d0.df34.32a3 Ethernet default-router 172.16.1.254

4.4.3 Configuring Global Properties of DHCP Server

Configuration Effect

Enable a server with specific functions, for example, ping and compulsory NAK.

Notes

Configuring the command may cause exceptions on other servers.

Configuration Steps

Configuring Excluded IP Address

- Optional. Configure some addresses or address ranges as unavailable.
- Run the **ip dhcp excluded-address** command in global configuration mode.

Configuring Compulsory NAK Reply

- Optional. A server replies to a wrong address request with a NAK packet.
- Run the **ip dhcp force-send-nak** command in global configuration mode.

Configuring VRRP Status Monitoring

- Optional. After configuration, DHCP packets are processed by the Master server.
- Run the **ip dhcp monitor-vrrp-state** command in global configuration mode.

Configuring Ping Times

- Optional. Check the address reachability with the **ping** command. The default is 2.
- Run the **ip dhcp ping packet** command in global configuration mode.

Configuring Ping Timeout

- Optional. Check the address reachability with the **ping** command. The default is 500 ms.
- Run the **ip dhcp ping timeout** command in global configuration mode.

Detecting User Offline Detection

- Configure a DHCP server to detect whether the client is offline or not. If a client does not get online after being offline for a period, the address assigned to the client will be retrieved.
- Run the **ip dhcp server arp-detect** command in global configuration mode.

Verification

Run the **dhcp-server** command, and check the configuration during address assignment.

Related Commands

Configuring Excluded IP Address

Command	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address:* Indicates a start IP address. *high-ip-address:* Indicates an end IP address.
Command Mode	Global configuration mode
Usage Guide	Unless otherwise specified, a DHCP server assigns all the addresses from an IP address pool to DHCP clients. To reserve some addresses(e.g., addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, it is recommended to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.

Configuring Compulsory NAK Reply

Command	**ip dhcp force-send-nak**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The server sends a NAK packet only when it finds the client's lease record. When a DHCP client crosses the network, a DHCP server cannot find lease record of the client and will not reply with a NAK packet. The client sends request packets continually before obtaining an IP address again after timeout. Consequently, it takes a long to obtain an IP address. This also occurs when a DHCP server loses a lease after restart and a client requests lease renewal. In this case, you may configure a command to force the DHCP server to reply with a NAK packet even though it cannot find the lease record so that the client may obtain an IP address rapidly. Please note that the command is disabled by default. To enable it, only one DHCP server can be configured in a broadcast domain.

Configuring Ping Times

Command	**ip dhcp ping packets** [*number*]

Parameter Description	*number:* (Optional) Ranges from 0 to 10. 0 indicates the ping function is disabled. The default is two pings.
Command Mode	Global configuration mode
Usage Guide	By default, when a DHCP server assigns an IP address from a pool, it runs the **Ping** command twice (one packet per time). If there is no reply, the server takes the address as idle and assigns it to a client. If there is a reply, the server takes the address as occupied and assigns another address.

Configuring Ping Timeout

Command	**ip dhcp ping timeout** *milliseconds*
Parameter Description	*milli-seconds:* Indicates the time that it takes for a DHCP server to wait for a ping reply. The value ranges from 100 ms to 10,000 ms.
Command Mode	Global configuration mode
Usage Guide	By default, if a DHCP server receives no Ping reply within 500 ms, the IP address is available. You may adjust the ping timeout to change the time for a server to wait for a reply.

Configuring ARP-Based Offline Detection

Command	**ip dhcp server arp-detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, DHCP server does not detect whether a client is offline or not based on ARP. After configuration, a DHCP server may perform the detection. If a client does not get online again after a period (5 minutes by default), a DHCP server retrieves the address assigned to the client.

Configuration Example

Configuring Ping

Configuration Steps	● Set ping times to 5. ● Set ping timeout to 800ms.
	Hostname(config)# ip dhcp ping packet 5 Hostname(config)# ip dhcp ping timeout 800
Verification	Run the **show run** command to display the configuration.
	Hostname(config)#show run | begin ip dhcp

	ip dhcp ping packet 5 ip dhcp ping timeout 800

Configuring Excluded IP Address

Configuration Steps	• Configure the excluded IP address from 192.168.0.0 to 192.168.255.255.
	Hostname(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
Verification	Run the **show run** command to display the configuration.
	Hostname(config)#show run | begin ip dhcp ip dhcp excluded-address 192.168.0.0 192.168.255.255

4.4.4 Configuring Basic DHCP Relay Functions

Configuration Effect

- Deploy dynamic IP management in Client–Relay–Server mode to achieve communication between a DHCP client and a DHCP server, which are in different network segments.

Notes

- To enable DHCP Relay, you need to configure IPv4 unicast routing in a network.

Configuration Steps

Enabling DHCP Relay

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Configuring IP Address for DHCP Server

- Mandatory.
- You need to configure an IP address for a DHCP server.

Verification

- Check whether a client obtains an IP address through DHCP Relay.

Related Commands

Enabling DHCP Relay

Command	**service dhcp**
Parameter Description	N/A
Comm	Global configuration mode

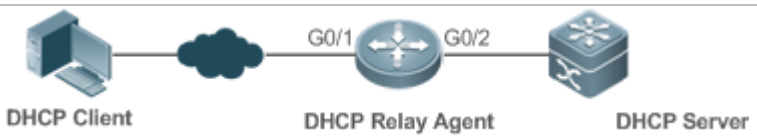
and Mode	
Usage Guide	N/A

Configuring IP Address for DHCP Server

Command	**ip helper-address { cycle-mode | *A.B.C.D* }**
Parameter Description	*cycle-mode*: Indicates that DHCP request packets are forwarded to all DHCP servers. *A.B.C.D*: Indicates the IP address of a server.
Command Mode	Global configuration mode/interface configuration mode
Usage Guide	You may configure the function on a layer-3 interface, such as a routed port, a L3 AP port, SVI and loopback interface. The configured interface must be accessible via IPv4 unicast routing.

Configuration Example

Configuring DHCP Relay in Wired Connection

Scenario Figure 4-10	
Configuration Steps	● Enable a client with DHCP to obtain an IP address. ● Enable the DHCP Relay function on a DHCP relay agent. ● Configure DHCP Server.
A	Enable a client with DHCP to obtain an IP address.

B	Enable DHCP Relay.
	`Hostname(config)# service dhcp`
	Configure a global IP address of a DHCP server.
	`Hostname(config)# ip helper-address 172.2.2.1`
	Configure an IP address for the port connected to the client.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if)# ip address 192.1.1.1 255.255.255.0`
	Configure an IP address for the port connected to the server.
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0`

C	Enable DHCP Server.
	`Hostname(config)# service dhcp`
	Configure an address pool.
	`Hostname(config)# ip dhcp pool relay`

	Hostname(dhcp-config)#network 192.1.1.0 255.255.255.0 Hostname(dhcp-config)#default-router 192.1.1.1 Configure an IP address for the port connected to the relay agent. Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
Verification	Check whether the client obtains an IP address. ● Check whether the client obtains an IP address. ● Check the DHCP Relay configuration.
A	The user device obtains an IP address.
B	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration. Hostname# show running-config service dhcp ip helper-address 172.2.2.1 ! interface GigabitEthernet 0/1 ip address 192.1.1.1 255.255.255.0 ! interface GigabitEthernet 0/2 ip address 172.2.2.2 255.255.255.0 !

Common Errors

- IPv4 unicast routing configuration is incorrect.
- DHCP Relay is disabled.
- No routing between DHCP relay agent and DHCP server is configured.
- No IP address is configured for the DHCP server.

4.4.5 Configuring DHCP Relay Option 82

Configuration Effect

- Through a DHCP relay agent, a server may assign IP addresses of different privileges to the clients more accurately based on the option information.

Notes

- You need to enable the DHCP Relay function.

Configuration Steps

↘ **Enabling Basic DHCP Relay Functions**

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Enables DHCP Option82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable or disable DHCP Option 82.

Verification

- Check whether the client obtains an IP address based on Option 82.

Related Commands

Enabling DHCP Option 82

Command	**ip dhcp relay information option82**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling DHCP Option 82

Configuration Steps	• Enable DHCP Option 82. • Configure sub-option commands.
	Hostname(config)# ip dhcp relay information option82
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Hostname#show ru | incl ip dhcp relay ip dhcp relay information option82

Common Errors

- Basic DHCP Relay functions are not configured.

4.4.6 Configuring DHCP Relay Check Server-ID

Configuration Effect

- After you configure the **ip dhcp relay check server-id**, a DHCP Relay agent will forward DHCP request packets only to the server specified by the **option server-id** command. Otherwise, they are forwarded to all DHCP servers.

Notes

- You need to enable basic DHCP Relay functions.

Configuration Steps

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Verification

Check whether a DHCP Relay agent sends DHCP request packets only to the server specified by the **option server-id** command.

Related Commands

Configuring DHCP Relay Check Server-ID

Command	**ip dhcp relay check server-id**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring DHCP Relay Check Server-ID

Configuration Steps	• Enable DHCP Relay. Omitted. • Enable **DHCP Relay check server-id** on an interface.
	Hostname# configure terminal Hostname(config)# ip dhcp relay check server-id
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Hostname# show running-config | include check server-id ip dhcp relay check server-id Hostname#

Common Errors

- Basic DHCP Relay functions are not configured.

4.4.7 Configuring DHCP Relay Suppression

Configuration Effect

- After you configure the **ip DHCP Relay suppression** command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP requests will be forwarded.

Notes

- You need to enable basic DHCP Relay functions.

Configuration Steps

Enabling DHCP Relay Suppression

By default, DHCP Relay suppression is disabled on all interfaces.

You may run the **ip dhcp relay suppression** command to enable DHCP Relay suppression.

Verification

- Check whether the DHCP request packets received on the interface are filtered.

Related Commands

Configuring DHCP Relay Suppression

Command	**ip dhcp relay suppression**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring DHCP Relay Suppression

Configuration Steps	• Configure basic DHCP Relay functions. • Configure DHCP Relay suppression on an interface.
	Hostname# configure terminal Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression Hostname(config-if-GigabitEthernet 0/1)#end Hostname#
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.

Configuration Steps	● Configure basic DHCP Relay functions. ● Configure DHCP Relay suppression on an interface.
	Hostname# configure terminal Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression Hostname(config-if-GigabitEthernet 0/1)#end Hostname#
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Hostname# show running-config | include relay suppression ip dhcp relay suppression Hostname#

Common Errors

Basic DHCP Relay functions are not configured.

4.4.8 Configuring DHCP Client

Configuration Effect

Enable DHCP Client on a device so that it obtains IP addresses and configurations dynamically.

Notes

Products support DHCP Client configuration on Ethernet, FR, PPP and HDLC interfaces.

Configuration Steps

Run the **ip address dhcp** command on an interface.

Verification

Check whether the interface obtains an IP address.

Related Commands

↘ **Configuring DHCP Client**

Command	**ip address dhcp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage	● Products support dynamic IP address obtainment by an Ethernet interface. ● Products support dynamic IP address obtainment by a PPP-encapsulated interface.

Guide	● Products support dynamic IP address obtainment by an FR-encapsulated interface. ● Products support dynamic IP address obtainment by an HDLC-encapsulated interface.

Configuration Example

Configuring DHCP Client

Configuration Steps	1: Enable port FastEthernet 0/0 with DHCP to obtain an IP address.
	Hostname(config)# interface FastEthernet0/0 Hostname(config-if-FastEthernet 0/0)#ip address dhcp
Verification	1: Run the **show run** command to display the configuration.
	Hostname(config)#show run | begin ip address dhcp ip address dhcp

4.5 Monitoring

Clearing

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

Description	Command
Clears DHCP address binding.	**clear ip dhcp binding** { *address* | *}
Clears DHCP address conflict.	**clear ip dhcp conflict** { *address* | *}
Clears statistics of a DHCP server.	**clear ip dhcp server statistics**
Clears statistics of a DHCP relay.	**clear ip dhcp relay statistics**
Clears statistics of DHCP server performance.	**clear ip dhcp server rate**

Displaying

Description	Command
Displays DHCP lease.	**show dhcp lease**
Displays DHCP sockets.	**show ip dhcp socket**
Displays assigned IP addresses.	**show ip dhcp binding**
Displays created address pools.	**show ip dhcp pool**
Displays statistics of DHCP Server.	**show ip dhcp server statistic**
Displays statistics of DHCP Relay.	**show ip dhcp relay statistic**

Displays conflicted addresses.	**show ip dhcp conflict**

Debugging



System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs DHCP agent.	**debug ip dhcp server agent**
Debugs DHCP hot backup.	**debug ip dhcp server ha**
Debugs DHCP address pools.	**debug ip dhcp server pool**
Debugs DHCP VRRP.	**debug ip dhcp server vrrp**
Debugs all DHCP servers.	**debug ip dhcp server all**
Debugs DHCP packets.	**debug ip dhcp client**
Debugs DHCP Relay events.	**debug ip dhcp relay**

5 Configuring DNS

5.1 Overview

A Domain Name System (DNS) is a distributed database containing mappings between domain names and IP addresses on the Internet, which facilitate users to access the Internet without remembering IP strings that can be directly accessed by computers. The process of obtaining an IP address through the corresponding host name is called domain name resolution (or host name resolution).

Protocols and Standards

- RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

5.2 Applications

Application	Description
Static Domain Name Resolution	Performs domain name resolution directly based on the mapping between a domain name and an IP address on a device.
Dynamic Domain Name Resolution	Obtains the IP address mapped to a domain name dynamically from a DNS server on the network.

5.2.1 Static Domain Name Resolution

Scenario

- Preset the mapping between a domain name and an IP address on a device.
- When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Deployment

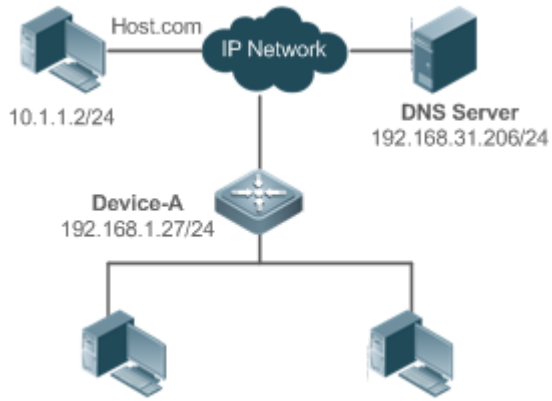
- Preset the mapping between a domain name and an IP address on a device.

5.2.2 Dynamic Domain Name Resolution

Scenario

- DNS Server is deployed on the network to provide the domain name service.
- Domain name "host.com" is deployed on the network.
- Device-A applies to DNS Server for domain name "host.com".

Figure 5-1 Dynamic Domain Name Resolution



Deployment

- Deploy DNS Server as the DNS server of Device-A.

5.3 Features

Basic Concepts

DNS

The DNS consists of a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on the network, and implements mutual conversion between the domain names and IP addresses. Both the TCP and UDP port IDs of DNS are 53, and generally a UDP port is used.

Features

Feature	Description
Domain Name Resolution	IP addresses are obtained based on domain names from a DNS server or a local database.

5.3.1 Domain Name Resolution

Working Principle

Static Domain Name Resolution

Static domain name resolution means that a user presets the mapping between a domain name and an IP address on a device. When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Dynamic Domain Name Resolution

Dynamic domain name resolution means that when a user perform domain name operations through application programs, the DNS resolver of the system queries an external DNS server for the IP address mapped to the domain name.

The procedure of dynamic domain name resolution is as follows:

9. A user application program (such as Ping or Telnet) requests the IP address mapped to a domain name from the DNS resolver of the system.
10. The DNS resolver queries the dynamic cache at first. If the domain name on the dynamic cache does not expire, the DNS resolver returns the domain name to the application program.
11. If all domain names expire, the DNS resolver initiates a request for domain name-IP address conversion to the external DNS server.

12. After receiving a response from the DNS server, the DNS resolver caches and transfers the response to the application program.

Related Configuration

Enabling Domain Name Resolution

- By default, domain name resolution is enabled.
- Run the **ip domain-lookup** command to enable domain name resolution.

Configuring the IP Address Mapped to a Static Domain Name

- By default, no mapping between a domain name and an IP address is configured.
- Run the **ip host** command to specify the IPv4 address mapped to a domain name.
- Run the **ipv6 host** command to specify the IPv6 address mapped to a domain name.

Configuring a DNS Server

- By default, no DNS server is configured.
- Run the **ip name-server** command to configure a DNS server.

5.4 Configuration

Configuration	Description and Command	
Configuring Static Domain Name Resolution	Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip host	Configures the IPv4 address mapped to a domain name.
	ipv6 host	Configures the IPv6 address mapped to a domain name.
Configuring Dynamic Domain Name Resolution	Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip name-server	Configures a DNS server.

5.4.1 Configuring Static Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name on a local device.

Configuration Steps

Enabling Domain Name Resolution

- The domain name resolution function is enabled by default.
- If this function is disabled, static domain name resolution does not take effect.

Configuring the IP Address Mapped to a Domain Name

- (Mandatory) Domain names to be used must be configured with mapped IP addresses.

Verification

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

- Run the **show hosts** command to check the mapping between the domain name and the IP address.

Related Commands

Configuring the IPv4 Address Mapped to a Domain Name

Command	**ip host** *host-name* [*telnet-port*] *ip-address*
Parameter Description	*host-name*: indicates a domain name. telnet-port: port number for telnet *ip-address*: indicates a mapped IPv4 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the IPv6 Address Mapped to a Domain Name

Command	**ipv6 host** *host-name* [*telnet-port*] *ipv6-address*
Parameter Description	*host-name*: indicates a domain name. telnet-port: port number for telnet *ipv6-address*: indicates a mapped IPv6 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Static Domain Name Resolution

Configuration Steps	• Set the IP address of static domain name www.test.com to 192.168.1.1 on a device. • Set the IP address of static domain name www.testv6.com to 2001::1 on a device.
	Hostname#configure terminal Hostname(config)# ip host www.test.com 192.168.1.1 Hostname(config)# ipv6 host www.testv6.com 2001::1 Hostname(config)# exit
Verification	Run the **show hosts** command to check whether the static domain name entry is configured.
	Hostname#show hosts Name servers are: Host type Address TTL(sec)

	www.test.com static 192.168.1.1 --- www.testv6.com static 2001::1 ---

5.4.2 Configuring Dynamic Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name through a DNS server.

Configuration Steps

Enabling Domain Name Resolution

- Domain name resolution is enabled by default.
- If this function is disabled, dynamic domain name resolution does not take effect.

Configuring a DNS Server

- (Mandatory) To use dynamic domain name resolution, you must configure an external DNS server.

Verification

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

Related Commands

Configuring a DNS Server

Command	**ip name-server** { *ip-address* | *ipv6-address* }
Parameter Description	*ip-address*: indicates the IPv4 address of the DNS server. *ipv6-address*: indicates the IPv6 address of the DNS server.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Dynamic Domain Name Resolution

Scenario Figure 5-2	
	Device resolves the domain name through the DNS server (192.168.10.1) on the network.
Configuration Steps	Set the IP address of the DNS server to 192.168.10.1 on the device.

	DEVICE#configure terminal DEVICE(config)# ip name-server 192.168.10.1 DEVICE(config)# exit
Verification	Run the **show hosts** command to check whether the DNS server is specified.
	Hostname(config)#show hosts Name servers are: 192.168.10.1 static Host type Address TTL(sec)

5.5 Monitoring

Clearing

Running the **clear** command during device operation may cause data loss or even interrupt services.

Description	Command
Clears the dynamic host name cache table.	**clear host** [*host-name*]

Displaying

Description	Command
Displays DNS parameters.	**show hosts** [*host-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the DNS function.	**debug ip dns**

6 Configuring TFTP Client

6.1 Overview

The Trivial File Transfer Protocol (TFTP) is an application of TCP/IP. TFTP transfers files between the client and server based on UDP. Compared with FTP based on TCP, TFTP does not require authentication and does not contain complex packets. TFTP applies to stable networks. TFTP is used to transfer small files whereas FTP is used to transfer large files.

Protocols and Standards

- RFC783: Trivial FILE TRANSFER PROTOCOL (TFTP)

6.2 Applications

Application	Description
Uploading a Local File to a Remote Server	Local and remote files need to be shared, for example, uploading a local file to a remote server.
Downloading a File from a Remote Server to a Local Device	Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

6.2.1 Uploading a Local File to a Remote Server

Scenario

Local and remote files need to be shared, for example, uploading a local file to a remote server.

As shown in Figure 6-1, resources are shared only on the Intranet.

Figure 6-1



Deployment

- Implement only communication on the Intranet.
- Enable file uploading on the TFTP client.

6.2.2 Downloading a File from a Remote Server to a Local Device

Scenario

Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

As shown in Figure 6-2, resources are shared only on the Intranet.

Figure 6-2



Deployment

- Implement only communication on the Intranet.
- Enable file downloading on the TFTP client.

6.3 Features

Basic Concepts

Uploading TFTP Files

Upload files from a TFTP client to a TFTP server.

Downloading TFTP Files

Download files from a TFTP server to a TFTP client.

Overview

Feature	Description
Uploading FTP Files	Uploads files from an FTP client to an FTP server.
Downloading FTP Files	Downloads files from an FTP server to an FTP client.

6.3.1 Uploading TFTP Files

TFTP enables file uploading. Start the TFTP client and TFTP server simultaneously, and upload files from the TFTP client to the FTP server.

6.3.2 Downloading TFTP Files

TFTP enables file downloading. Start the TFTP client and TFTP server simultaneously, and download files from the TFTP server to the TFTP client.

6.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	(Mandatory) It is used to configure the functions of an FTP client.	
	copy flash	Uploads a file.
	copy ftp	Downloads a file.

6.4.1 Configuring Basic Functions

Configuration Effect

- Implement file uploading and downloading.

Notes

- Pay attention to the command formats for uploading and downloading.

Configuration Steps

Uploading a File

- This configuration is mandatory when a file needs to be uploaded.
- Configure the TFTP URL as the destination address of **copy** in Privileged EXEC mode.

Downloading a File

- This configuration is mandatory when a file needs to be downloaded.
- Configure the TFTP URL as the source address of **copy** in Privileged EXEC mode.

Verification

- Check whether the uploaded file exists on the TFTP server.
- Check whether the downloaded file exists at the destination address.

Related Commands

Uploading a File

Command	**copy flash:**[*local-directory/*]*local-file* **tftp:** *// dest-address*[*/remote-directory*]*/remote-file*
Parameter Description	*local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory. *local-file:* Specifies a local file to be uploaded. *dest-address:* Specifies an IP address for the FTP server. *remote-directory:* Specifies a directory on the server. *remote-file:* Renames the file on the server. ⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to upload a file from the flash of a local device to an FTP server.

Downloading an FTP File

Command	**copy tftp://** *dest-address*[*/remote-directory*]*/remote-file* **flash:**[*local-directory/*]*local-file*
Parameter Description	*dest-address:* Specifies an IP address for the FTP server. *remote-directory:* Specifies a directory on the server. *remote-file:* Specifies a file to be downloaded. *local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory. *local-file:* Renames the file in the local flash. ⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to download a file from a TFTP server to the flash of a local device.

Configuration Example

Uploading a File

Configuration Steps	Upload the **local-file** file in the **flash** directory of a device to the **root** directory of a TFTP server whose IP address is **192.168.23.69** and name the file as **remote-file**.
	`Hostname# copy flash: home/local-file tftp:// 192.168.23.69/root/remote-file`
Verification	Check whether the **remote-file** file exists on the TFTP server.

Downloading a File

Configuration Steps	Download the **remote-file** file from the **root** directory of a TFTP server whose IP address is **192.168.23.69** to the **home** directory of a device and save the file as **local-file**.
	`Hostname# copy Tftp:// 192.168.23.69/root/remote-file flash: home/local-file`
Verification	Check whether the **remote-file** file exists in the **home** directory of the flash.

Common Errors

- The command formats for uploading and downloading are incorrect.
- The user name or password is incorrect.

6.5 Monitoring

Displaying

Description	Command

Displays the TFTP client configuration.	**show run**

Debugging



System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the TFTP Client.	**debug tftp**

7 Configuring Network Communication Test Tools

7.1 Overview

Network communication test tools can be used to check the connectivity of a network and helps you analyze and locate network faults. Network communication test tools include Packet Internet Groper (PING) and Traceroute. Ping is used to check the connectivity and delay of a network. A greater delay indicates a slower network speed. Traceroute helps you learn about the topology of physical and logical links and transmission rate. On a network device, you can run the **ping** and **traceroute** commands to use the two tools respectively.

Protocols and Standards

- RFC792: Internet Control Message Protocol
- RFC4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

7.2 Applications

Application	Description
End-to-End Connectivity Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.
Host Route Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.

7.2.1 End-to-End Connectivity Test

Scenario

As shown in Figure 7-1, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the end-to-end connectivity test aims to check whether IP packets can be transmitted between the two ends. The target host can be the network device itself. In this case, the connectivity test aims to check the network interface and TCP/IP configurations on the device.

Figure 7-1



Deployment

Execute the ping function on the network device.

7.2.2 Host Route Test

Scenario

As shown in Figure 7-2, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the host route test aims to check gateways (or routers) that IP packets pass through between the two ends. Generally, the target host is not within the same IP network segment as the network device.

Figure 7-2



Deployment

Execute the traceroute function on the network device.

7.3 Features

Overview

Feature	Description
Ping Test	Test whether the specified IPv4 or IPv6 address is reachable and display the related information.
Traceroute Test	Display the gateways that IPv4 or IPv6 packets pass through when transmitted from the source to the destination.

7.3.1 Ping Test

Working Principle

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request the for an ICMP Echo Reply message. In this way, the ping tool determines the delay and the connectivity between the two network devices.

Related Configuration

- Run the **ping** command.

7.3.2 Traceroute Test

Working Principle

The traceroute tool uses the Time To Live (TTL) field in the headers of the ICMP and IP messages for the test First, the traceroute tool on the network device sends an ICMP Request message with TTL 1 to the destination host. After receiving the message, the first router on the path decreases the TTL by 1. As the TTL becomes 0, the router drops the packets and returns an ICMP time exceeded message to the network device. After receiving this message, the traceroute tool learns that this router exists on this path, and then sends an ICMP Request packet with TTL 2 to the destination host to discover the second router. Each time the traceroute tool increases the TTL in the ICMP Request message by 1 to discover one more router. This process is repeated until a data packet reaches the destination host. After the packet reaches the destination host, the host returns an ICMP Echo message instead of an ICMP time exceeded message to the network device. Then, the traceroute tool finishes the test and displays the path from the network device to the destination host.

Related Configuration

- Run the **traceroute** command.

7.4 Configuration

Configuration	Description and Command

Ping Test	(Optional) It is used to check whether an IPv4 or IPv6 address is reachable.	
	ping	Executes the Ping function.
Traceroute Test	(Optional) It is used to display the gateways that IPv4 or IPv6 packets pass through when transmitted from the source to the destination.	
	traceroute	Executes the traceroute function.

7.4.1 Ping Test

Configuration Effect

After conducting a ping test on a network device, you can learn whether the network device is connected to the destination host and whether packets can be transmitted between the network device and the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To check whether an IPv4 address is reachable, use the **ping IPv4** command.
- To check whether an IPv6 address is reachable, use the **ping IPv6** command.

Verification

Run the **ping** command to display related information on the command line interface (CLI) window.

Related Commands

Ping IPv4

Command	**ping** [**ip**] *address* [**data** *data*] [**detail**] [**df-bit**] [**interval** millisecond] [**length** *length*] [**ntimes** *times*] [**source** *source*] [**timeout** *seconds*] [**validate**]
Parameter Description	*address*: Specifies the destination IPv4 address or domain name. **data** *data*: Specifies the data in the packet. The data is a string of 1 to 255 bytes. By default, the string is "abcd". **detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. **df-bit**: Configures the DF bit of the IP address. When the DF bit is set to 1, the packet is not fragmented. By default, the DF bit is 0. **interval** millisecond: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms. **length** *length*: Specifies the length of the data packet. The value ranges from 36 to 18, 024. The default length is 100. **ntimes** *times*: Specifies the number of probes. The value ranges from 1 to 4, 294, 967, 295 **source** *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. **timeout** *seconds*: Specifies the timeout. The value ranges from 1s to 10s. **validate**: Configures whether to verify the response packet.
Command Mode	In User EXEC mode, you can execute only the basic ping function. In Privileged EXEC mode, you can execute the extended ping function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping function, you can specify the number, length and timeout of packets to be sent. Like the basic ping function, related statistics will be output. To use the domain name, you must first configure the domain name server (DNS). For details about

	the configuration, see *Configuring DNS*.

Ping IPv6

Command	**ping ipv6** *ipv6-address* [**data** *data*] [**detail**] [**interval** millisecond] [**length** *length*] [**ntimes** *times*] [**source** *source*] [**timeout** *seconds*]
Parameter Description	*ipv6-address*: Specifies the destination IPv6 address or domain name. **data** *data*: Specifies the data in the packet. The data is a string of 1 to 255 bytes. **detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. **interval** millisecond: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms. **length** *length*: Specifies the length of data packet. The value ranges from 16 to 18, 024. The default length is 100. **ntimes** *times*: Specifies the number of probes. The value ranges from 1 to 4, 294, 967, 295. **source** *source*: Specifies the source IPv6 address or source port of the packet. The loopback interface address, for example, ::1, cannot be used as the source address. **timeout** *seconds*: Specifies the timeout. The value ranges from 1s to 10s.
Command Mode	In User EXEC mode, you can execute only the basic ping IPv6 function. In Privileged EXEC mode, you can execute the extended ping IPv6 function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping IPv6 function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping IPv6 function, you can specify the number, length and timeout of packets to be sent. Like the basic ping IPv6 function, related statistics will be output. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Common Ping Function

Configuration Steps	In Privileged EXEC mode, run the **ping 192.168.21.26** command.
	Common ping command: Hostname# ping 192.168.21.26 Sending 5, 100-byte ICMP Echoes to 192.168.21.26, 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 Detailed ping command: Hostname#ping 192.168.21.26 detail Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break >

	Reply from 192.168.21.26: bytes=100 time=4ms TTL=64 Reply from 192.168.21.26: bytes=100 time=3ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping Function

Configuration Steps	In Privileged EXEC mode, run the **ping 192.168.21.26** command. In addition, specify the length, number, and timeout of the packets.
	Common ping command: Hostname# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3 Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, 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 Detailed ping command: ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.
Verification	Send twenty 1500-byte packets to the specified IP address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

Executing the Common Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the **ping ipv6 2001::1** command.
	Common ping command: Hostname# ping ipv6 2001::1 Sending 5, 100-byte ICMP Echoes to 2001::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 Detailed ping command: Hostname#ping 2001::1 detail Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > Reply from 2001::1: bytes=100 time=1ms

	Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the **ping ipv6 2001::5** command. In addition, specify the length, number, and timeout of the packets.
	Common ping command: Hostname# ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3 Sending 100, 1500-byte ICMP Echoes to 2000::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 Detailed ping command: Hostname#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3 Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds: < press Ctrl+C to break > Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms

	Reply from 2001::5: bytes=1500 time=1ms Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
Verification	Send one hundred 1500-byte packets to the specified IPv6 address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

7.4.2 Traceroute Test

Configuration Effect

After conducting a traceroute test on a network device, you can learn about the routing topology between the network device and the destination host, and the gateways through which packets are sent from the network device to the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To trace the route an IPv4 packet would follow to the destination host, run the **traceroute IPv4** command.
- To trace the route an IPv6 packet would follow to the destination host, run the **traceroute IPv6** command.

Verification

Run the **traceroute** command to display related information on the CLI window.

Related Commands

Traceroute IPv4

Command	**traceroute** [**ip**] *ipv4-adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]
Parameter Description	*Ipv4-address*: Specifies the destination IPv4 address or domain name. **probe** *number*: Specifies the number of probes. The value ranges from 1 to 255. **source** *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. **timeout** *seconds*: Specifies the timeout. The value ranges from 1s to 10s. **ttl** *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.
Command Mode	In User EXEC mode, you can execute only the basic traceroute function. In privileged EXEC mode, you can execute the extended traceroute function.
Configuration Usage	The **traceroute** command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Traceroute IPv6

Command	**traceroute** [**ipv6** *address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]

Parameter Description	*ipv6-address*: Specifies the destination IPv6 address or domain name. **probe** *number*: Specifies the number of probes. The value ranges from 1 to 255. **timeout** *seconds*: Specifies the timeout. The value ranges from 1s to 10s. **ttl** *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.
Command Mode	In User EXEC mode, you can execute only the basic traceroute IPv6 function. In privileged EXEC mode, you can execute the extended traceroute IPv6 function.
Configuration Usage	The traceroute IPv6 command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Traceroute Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.
	Hostname# Hostname# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–3. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute 202.108.37.42** command.

```
Hostname# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1       192.168.12.1        0 msec  0 msec  0 msec
2       192.168.9.2         0 msec  4 msec 4 msec
3       192.168.110.1      16 msec  12 msec  16 msec
4       *  *  *
5       61.154.8.129        12 msec  28 msec  12 msec
6       61.154.8.17          8 msec  12 msec  16 msec
7       61.154.8.250        12 msec  12 msec  12 msec
8       218.85.157.222      12 msec  12 msec  12 msec
9       218.85.157.130      16 msec  16 msec  16 msec
10      218.85.157.77       16 msec  48 msec  16 msec
11      202.97.40.65        76 msec  24 msec  24 msec
12      202.97.37.65        32 msec  24 msec  24 msec
13      202.97.38.162       52 msec  52 msec  224 msec
14      202.96.12.38        84 msec  52 msec  52 msec
15      202.106.192.226     88 msec  52 msec  52 msec
16      202.106.192.174     52 msec  52 msec  88 msec
17      210.74.176.158     100 msec  52 msec  84 msec
18      202.108.37.42       48 msec  48 msec  52 msec
```

The preceding test result indicates that the network device accesses host 202.108.37.42 by transmitting packets through gateways 1–17, and Gateway 4 is faulty.

Executing the Traceroute IPv6 Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.

	Hostname# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1-4. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute IPv6 Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.
	Hostname# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 * * * 5 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–5, and Gateway 4 is faulty.

8 Configuring TCP

8.1 Overview

The Transmission Control Protocol (TCP) is a transport-layer protocol providing reliable connection-oriented and IP-based services to for the application layer.

Internetwork data flows in 8-bit bytes are sent from the application layer to the TCP layer, and then fragmented into packet segments of a proper length via the TCP. The Maximum Segment Size (MSS) is usually limited by the Maximum Transmission Unit (MTU) of the data link layer. After that, the packets are sent to the IP layer and then to the TCP layer of a receiver through the network.

To prevent packet loss, every byte is identified by a sequence number via the TCP, and this ensures that packets destined for the peer are received in order. Then, the receiver responds with a TCP ACK packet upon receiving a packet. If the sender does not receive ACK packets in a reasonable Round-Trip Time (RTT), the corresponding packets (assumed lost) will be retransmitted.

- TCP uses the checksum function to check data integrity. Besides, MD5-based authentication can be used to verify data.
- Timeout retransmission and piggyback mechanism are adopted to ensure reliability.
- The Sliding Window Protocol is adopted to control flows. As documented in the Protocol, unidentified groups in a window should be retransmitted.

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 4022: Management Information Base for the Transmission Control Protocol (TCP)

8.2 Applications

Application	Description
Optimizing TCP Performance	To avoid TCP packet fragmentation on a link with a small MTU, Path MTU Discovery (PMTUD) is enabled.
Detecting TCP Connection Exception	TCP checks whether the peer works normally.

8.2.1 Optimizing TCP Performance

Scenario

For example, TCP connection is established between A and D, as shown in the following figure. The MTU of the link between A and B is 1500 bytes, 1300 bytes between B and C, and 1500 bytes between C and D. To optimize TCP transmission performance, packet fragmentation should be avoided between B and C.

Figure 8-1



Remarks:	A, B, C and D are routers.

Deployment

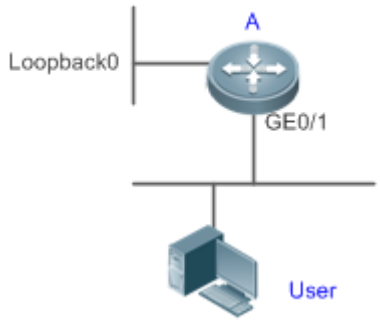
- Enable PMTUD on A and D.

8.2.2 Detecting TCP Connection Exception

Scenario

For example, in the following figure, User logs in to A through telnet but is shut down abnormally, as shown in the following figure. In case of TCP retransmission timeout, the User's TCP connection remains for a long period. Therefore, TCP keepalive can be used to rapidly detect TCP connection exception.

Figure 8-2



Remarks:	A is a router.

Deployment

- Enable TCP keepalive on A.

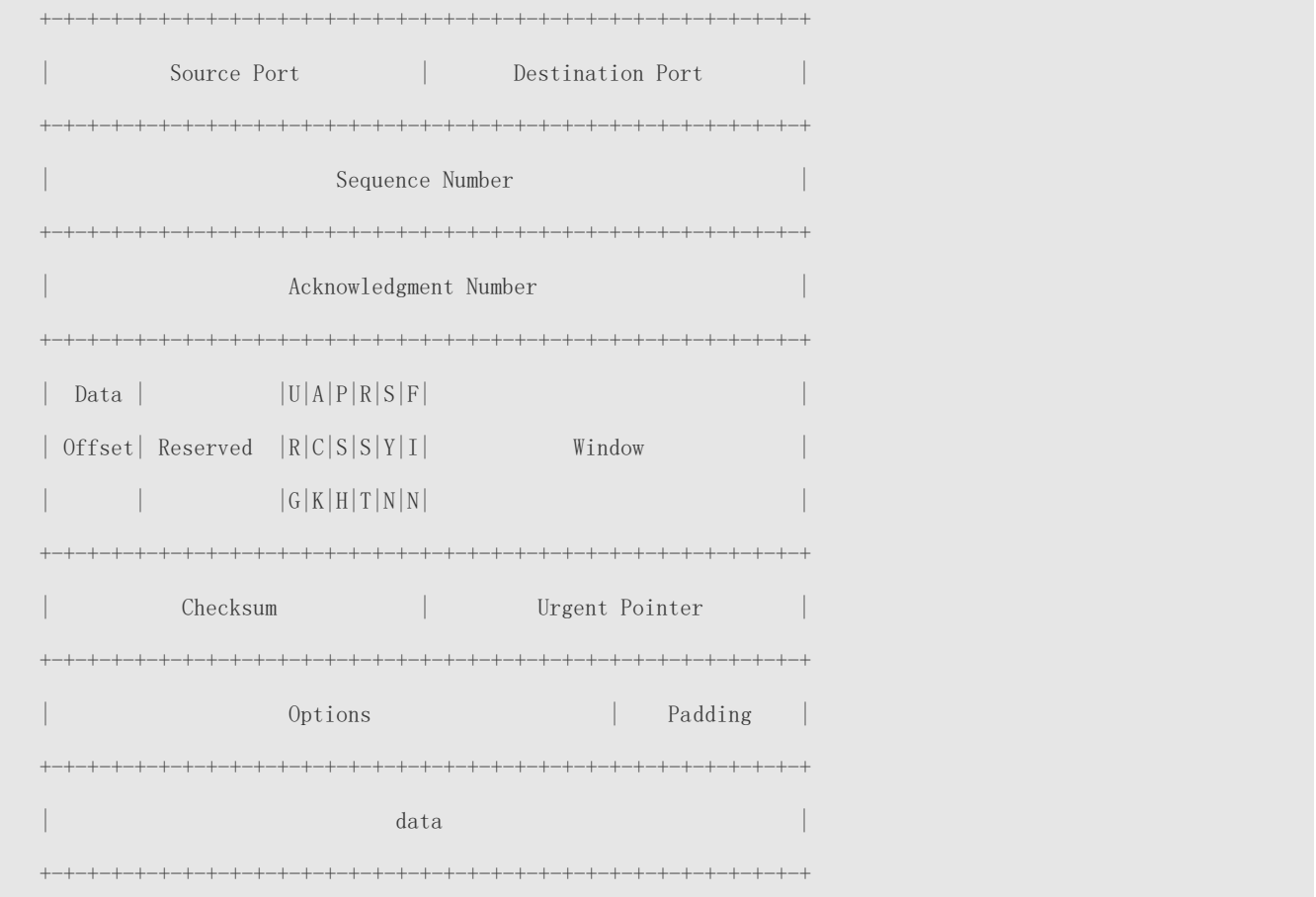
8.3 Features

Basic Concepts

TCP Header Format

```
0                   1                   2                   3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



- **Source Port** is a 16-bit source port number.
- **Destination Port** is a 16-bit destination port number.
- **Sequence Number** is a 32-bit sequence number.
- **Acknowledgment Number** is a 32-bit number that identifies the next sequence number that the receiver is expecting to receive.
- **Data Offset** is a 4-bit number that indicates the total number of bytes in the TCP header (option included) divided by 4.
- A flag bit is 6-bit. URG: the urgent pointer field is significant; ACK: the acknowledgment field is significant; PSH: indicates the push function; RST: resets TCP connection; SYN: synchronizes the sequence number (establishing a TCP connection); FIN: no more data from the sender (closing a TCP connection).
- A 16-bit Window value is used to control flows. It specifies the amount of data that may be transmitted from the peer between ACK packets.
- **Checksum** is a 16-bit checksum.
- **Urgent Pointer** is 16-bit and shows the end of the urgent data so that interrupted data flows can continue. When the U bit is set, the data is given priority over other data flows.

TCP Three-Way Handshake

- The process of TCP three-way handshake is as follows:

13. A client sends a SYN packet to the server.
14. The server receives the SYN packet and responds with a SYN ACK packet.
15. The client receives the SYN packet from the server and responds with an ACK packet.

- After the three-way handshake, the client and server are connected successfully and ready for data transmission.

Overview

Feature	Description
Configuring SYN Timeout	Configure a timeout waiting for a response packet after an SYN or SYN ACK packet is sent.
Configuring Window Size	Configure a window size.
Configuring Reset Packet Sending	Configure the sending of TCP reset packets after receiving port unreachable messages.
Configuring MSS	Configure an MSS for TCP connection.
Path MTU Discovery	Discover the smallest MTU on TCP transmission path, and adjust the size of TCP packets based on this MTU to avoid fragmentation.
TCP Keepalive	Check whether the peer works normally.

8.3.1 Configuring SYN Timeout

Working Principle

A TCP connection is established after three-way handshake: The sender sends an SYN packet, the receiver replies with a SYN ACK packet, and then the sender replies with an ACK packet.

- If the receiver does not reply with a SYN ACK packet after the sender sends an SYN packet, the sender keeps retransmitting the SYN packet for certain times or until timeout period expires.
- If the receiver replies with a SYN ACK packet after the sender sends an SYN packet but the sender does not reply with an ACK packet, the receiver keeps retransmitting the SYN ACK packet for certain times or until timeout period expires. (This occurs in the case of SYN flooding.)

Related Configuration

↘ Configuring TCP SYN Timeout

- The default TCP SYN timeout is 20 seconds.
- Run the **ip tcp synwait-time** *seconds* command in global configuration mode to configure an SYN timeout ranging from 5 to 300 seconds.

8.3.2 In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout Configuring Window Size

Working Principle

Data from the peer is cached in the TCP receiving buffer and subsequently read by applications. The TCP window size indicates the size of free space of the receiving buffer. For wide-bandwidth bulk-data connection, enlarging the window size dramatically promotes TCP transmission performance.

Related Configuration

↘ Configuring Window Size

- Run the **ip tcp window-size** *size* command in global configuration mode to configure a window size ranging from 128 to (65535<< 14) bytes. The default is 65535 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 smaller value between the configured window size and the free space of the receiving buffer.

8.3.3 Configuring Reset Packet Sending

Working Principle

When TCP packets are distributed to applications, if the TCP connection a packet belongs to cannot be identified, the local end sends a reset packet to the peer to terminate the TCP connection. Attackers may use port unreachable messages to attack the device.

Related Configuration

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Run the **no ip tcp send-reset** command in global configuration mode to disable TCP reset packet sending upon receiving port unreachable messages.

After this function is enabled, attackers may use port unreachable messages to attack the device.

8.3.4 Configuring MSS

Working Principle

The MSS refers to the total amount of data contained in a TCP segment t excluding TCP options.

Three-way handshake is implemented through MSS negotiation. Both parties add the MSS option to SYN packets, indicating the largest amount of data that the local end can handle, namely, the amount of data allowed from the peer. Both parties take the smaller MSS between them as the advertised MSS.

The MSS value is calculated as follows:

- IPv4 TCP: MSS = Outgoing interface MTU –IP header size (20-byte)–TCP header size (20-byte).
- IPv6 TCP: MSS = IPv6 Path MTU –IPv6 header size (40-byte)–TCP header size (20-byte).

The effective MSS is the smaller one between the calculated MSS and the configured MSS.

If a connection supports certain options, the option length (with **data offset** taken into consideration) should be deducted from an MSS value. For example, 20 bytes for MD5 digest (with **data offset** taken into consideration) should be subtracted from the MSS.

Related Configuration

Configuring MSS

- Run the **ip tcp mss** *max-segment-size* command in global configuration mode to set an MSS. It ranges from 68 to 1000 bytes. By default, the MSS is calculated based on MTU. If an MSS is configured, the effective MSS is the smaller one between the calculated MSS and the configured MSS.
- An excessively small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Choose an MSS value by referring to the interface MTU. If the former is bigger, TCP packets will be fragmented and transmission performance will be reduced.

8.3.5 Path MTU Discovery

Working Principle

The Path MTU Discovery f stipulated in RFC1191 is used to discover the smallest MTU in a TCP path to avoid fragmentation, enhancing network bandwidth utilization. The process of TCPv4 Path MTU Discovery is described as follows:

1. The source sends TCP packets with the Don't Fragment (DF) bit set in the outer IP header.
2. If the outgoing interface MTU value of a router in the TCP path is smaller than the IP packet length, the packet will be discarded and an ICMP error packet carrying this MTU will be sent to the source.
3. Through parsing the ICMP error packet, the source knows the smallest MTU in the path (path MTU) is.
4. The size of subsequent data segments sent by the source will not surpass the MSS, which is calculated as follows: TCP MSS = Path MTU – IP header size – TCP header size.

Related Configuration

Enabling Path MTU Discovery

By default, Path MTU Discovery is disabled.

Run the **ip tcp path-mtu-discovery** command to enable PMTUD in global configuration mode.

8.3.6 TCP Keepalive

Working Principle

You may enable TCP keepalive to check whether the peer works normally. If a TCP end does not send packets to the other end for a period of time (namely idle period), the latter starts sending keepalive packets successively to the former for several times. If no response packet is received, the TCP connection is considered inactive and then closed.

Related Configuration

Enabling Keepalive

- By default, TCP keepalive is disabled.
- Run the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command to in global configuration mode to enable TCP keepalive. See **Configuration** for parameter description.

8.4 Configuration

Configuration	Description and Command	
Optimizing TCP Performance	(Optional) It is used to optimize TCP connection performance.	
	ip tcp synwait-time	Configures a timeout for TCP connection.
	ip tcp window-size	Configures a TCP window size.
	ip tcp send-reset	Configures the sending of TCP reset packets after receiving port unreachable messages.
	ip tcp mss	Configures an MSS for TCP connection.
	ip tcp path-mtu-discovery	Enables Path MTU Discovery.
Detecting TCP Connection	(Optional) It is used to detect whether the peer works normally.	

Exception	**ip tcp keepalive**	Enables TCP keepalive.

8.4.1 Optimizing TCP Performance

Configuration Effect

- Ensure optimal TCP performance and prevent fragmentation.

Notes

N/A

Configuration Steps

Configuring SYN Timeout

- Optional.
- Configure this on the both ends of TCP connection.

Configuring TCP Window Size

- Optional.
- Configure this on the both ends of TCP connection.

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages.

- Optional.
- Configure this on the both ends of TCP connection.

Configuring MSS

- Optional.
- Configure this on the both ends of TCP connection.

Enabling Path MTU Discovery

- Optional.
- Configure this on the both ends of TCP connection.

Verification

N/A

Related Commands

Configuring SYN Timeout

Command	**ip tcp synwait-time** *seconds*
Parameter Description	*seconds*: Indicates SYN packet timeout. It ranges from 5 to 300 seconds. The default is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time.

	You may prolong SYN timeout properly on a poor network.

Configuring TCP Window Size

Command	**ip tcp window-size** *size*
Parameter Description	*size*: Indicates a TCP window size. It ranges from 128 to (65535 << 14) bytes. The default is 65535 bytes.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

Command	**ip tcp send-reset**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Configuring MSS

Command	**ip tcp mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size. It ranges from 68 to 10000 bytes. By default, the MSS is calculated based on MTU.
Command Mode	Global configuration mode
Usage Guide	This command defines the MSS for a TCP communication to be established. The negotiated MSS for a new connection should be smaller than this MSS. If you want to reduce the MSS, run this command. Otherwise, do not perform the configuration.

Configuring Path MTU Discovery

Command	**ip tcp path-mtu-discovery** [**age-timer** *minutes* **| age-timer infinite**]
Parameter Description	**age-timer** *minutes*: Indicates the interval for a new probe after a path MTU is discovered. It ranges from 10 to 30 minutes. The default is 10 minutes. **age-timer infinite**: No probe is implemented after a path MTU is discovered.
Command Mode	Global configuration mode
Usage Guide	The PMTUD is an algorithm documented in RFC1191 aimed to improve bandwidth utilization.

	When the TCP is applied to bulk data transmission, this function may facilitate transmission performance. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The age timer is a time interval for how often TCP estimates the path MTU with a larger MSS. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You may turn off the timer by setting it to **infinite**.

Configuration Example

↘ Enabling Path MTU Discovery

Configuration Steps	Enable PMTUD for a TCP connection. Adopt the default age timer settings.

	`Hostname# configure terminal`
	`Hostname(config)# ip tcp path-mtu-discovery`
	`Hostname(config)# end`

Verification	Run the **show tcp pmtu** command to display the IPv4 TCP PMTU.

	`Hostname# show tcp pmtu`
	`Number Local Address Foreign Address PMTU`
	`1 192.168.195.212.23 192.168.195.112.13560 1440`

	Run the **show ipv6 tcp pmtu** command to display the IPv6 TCP PMTU.

	`Hostname# show ipv6 tcp pmtu`
	`Number Local Address Foreign Address PMTU`
	`1 1000::1:23 1000::2.13560 1440`

Common Errors

N/A

8.4.2 Detecting TCP Connection Exception

Configuration Effect

- Check whether the peer works normally.

Notes

N/A

Configuration Steps

↘ Enabling TCP Keepalive

- Optional.

Verification

N/A

Related Commands

Enabling TCP Keepalive

Command	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]
Parameter Description	**interval** *num1*: Indicates the interval to send keepalive packets. Ranging from 1 to120 seconds. The default is 75 seconds. **times** *num2*: Indicates the maximum times for sending keepalive packets. It ranges from 1 to 10. The default is 6. **idle-period** *num3*: Indicates the time when the peer sends no packets to the local end, It ranges from 60 to 1800 seconds. The default is15 minutes.
Command Mode	Global configuration mode
Usage Guide	You may enable TCP keepalive to check whether the peer works normally. The function is disabled by default. Suppose a user enables TCP keepalive function with the default interval, times and idle period settings. The user does not receive packets from the other end within 15 minutes and then starts sending Keepalive packets every 75 seconds for 6 times. If the user receives no TCP packets, the TCP connection is considered inactive and then closed.

Configuration Example

Enabling TCP Keepalive

Configuration Steps	Enable TCP keepalive on a device with **interval** and **idle-period** set to 3 minutes and 60 seconds respectively. If the user receives no TCP packets from the other end after sending keepalive packets four times, the TCP connection is considered inactive.
	Hostname# configure terminal Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180 Hostname(config)# end
Verification	A user logs in to a device through telnet, and then shuts down the local device. Run the **show tcp connect** command on the remote device to observe when IPv4 TCP connection is deleted.

Common Errors

N/A

8.5 Monitoring

Displaying

Description	Command
Displays basic information on IPv4 TCP connection.	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP connection statistics.	**show tcp connect statistics**

Description	Command
Displays IPv4 TCP PMTU.	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP port information.	**show tcp port** [*num*]
Displays IPv4 TCP parameters.	**show tcp parameter**
Displays IPv4 TCP statistics.	**show tcp statistics**
Displays basic information on IPv6 TCP connection.	**show ipv6 tcp connect** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP connection statistics.	**show ipv6 tcp connect statistics**
Displays IPv6 TCP PMTU.	**show ipv6 tcp pmtu** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP port information.	**show ipv6 tcp port** [*num*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Displays the debugging information on IPv4 TCP packets.	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv4 TCP connection.	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]
Displays the debugging information on IPv6 TCP packets.	**debug ipv6 tcp packet** [**in** | **out**] [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv6 TCP connection.	**debug ipv6 tcp transactions** [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]

9 Configuring IPv4/IPv6 REF

9.1 Overview

On products incapable of hardware-based forwarding, IPv4/IPv6 packets are forwarded through the software. To optimize the software-based forwarding performance, the IPv4/IPv6 express forwarding through software is introduced.

REF maintains two tables: forwarding table and adjacency table. The forwarding table is used to store route information. The adjacency table is derived from the ARP table and IPv6 neighbor table, and it contains Layer 2 rewrite(MAC) information for the next hop..

REF is used to actively resolve next hops and implement load balancing.

Protocols and Standards

N/A

9.2 Applications

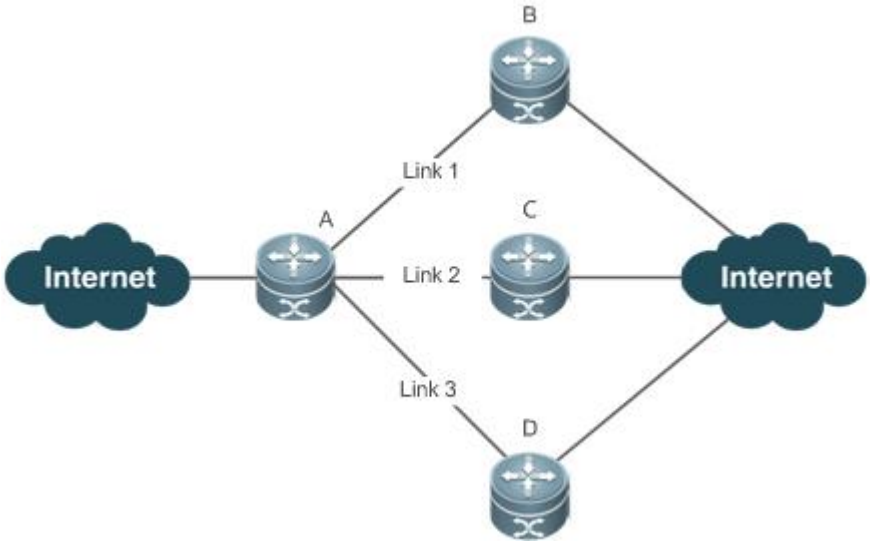
Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among the multiple next hops.

9.2.1 Load Balancing

Scenario

As shown in Figure 9-1, a route prefix is associated with three next hops on router A, namely, link 1, link 2, and link 3. By default, REF implements load balancing based on the destination IP address. Load balancing can be implemented based on the source IP address and destination IP address as well.

Figure 9-1



R	A is a router that runs REF.

Remarks	B, C and D are forwarding devices.

Deployment

- Run REF on router A.

9.3 Features

Basic Concepts

IPv4/IPv6 REF involves the following basic concepts:

Routing table

An IPv4/IPv6 routing table stores routes to the specific destinations and contains the topology information. During packet forwarding, IPv4/IPv6 REF selects packet transmission paths based on the routing table.

Adjacent node

An adjacent node contains output interface information about routed packets, for example, the next hop, the next component to be processed, and the link layer encapsulation. When a packet is matched with an adjacent node, the packet is directly encapsulated and then forwarded. For the sake of query and update, an adjacent node table is often organized into a hash table. To support routing load balancing, the next hop information is organized into a load balance entry. An adjacent node may not contain next hop information. It may contain indexes of next components (such as other line cards and multi-service cards) to be processed.

Active resolution

REF supports next hop resolution. If the MAC address of the next hop is unknown, REF will actively resolve the next hop. IPv4 REF requests the ARP module for next hop resolution while IPv6 REF applies the ND module to resolution.

Packet forwarding path

Packets are 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 determined.

9.3.1 Load Balancing Policies

Load balancing is configured to distribute traffic load among multiple network links.

Working Principle

REF supports two load balancing modes. In the REF model, a route prefix is associated with multiple next hops, in other words, it is a multi-path route. The route will be associated with a load balance table and implement weight-based load balancing. When an IPv4/IPv6 packet is matched with a load balance entry based on the longest prefix match, REF performs hash calculation based on the IPv4/IPv6 address of the packet and selects a path to forward the packet.

IPv4/IPv6 REF supports two kinds of load balancing policies: load balancing based on destination IP address, and load balancing based on the source and destination IP addresses.

Related Configuration

N/A

9.4 Monitoring

Displaying REF Packet Statistics

REF packet statistics includes the number of forwarded packets and the number of packets discarded due to various causes. You can determine whether packets are forwarded as expected by displaying and clearing REF packet statistics.

Command	Description
show ip ref packet statistics	Displays IPv4 REF packet statistics.
clear ip ref packet statistics	Clears IPv4 REF packet statistics.
show ipv6 ref packet statistics	Displays IPv6 REF packet statistics.
clear ipv6 ref packet statistics	Clears IPv6 REF packet statistics.

Displaying Adjacency Information

You can run the following commands to display adjacency information:

Command	Description
show ip ref adjacency [**glean** | **local** | *ip-address* | {**interface** *interface_type interface_number* } **| discard | statistics**]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes in IPv4 REF.
show ipv6 ref adjacency [glean | local | *ipv6-address* **| {interface** *interface_type interface_number}* **| discard | statistics**]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IPv6 address, adjacencies associated with a specified interface, and all adjacent nodes in IPv6 REF.

Displaying Active Resolution Information

You can run the following commands to display next hops to be resolved:

Command	Description
show ip ref resolve-list	Displays the next hop to be resolved .
show ipv6 ref resolve-list	Displays the next hop to be resolved.

Displaying Packet Forwarding Path Information

Packets are 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 determined. Run the following commands and specify the IPv4/IPv6 source and destination addresses of a packet. The forwarding path of the packet is displayed, for example, the packet is discarded, submitted to a CPU, or forwarded. Furthermore, the interface that forwards the packet is displayed.

Command	Description
show ip ref exact-route *source-ipaddress dest_ipaddress*	Displays the forwarding path of a packet.
show ipv6 ref exact-route *src-ipv6-address dst-ipv6-address*	Displays the forwarding path of an IPv6 packet.

Displaying Route Information in an REF Table

Run the following commands to display the route information in an REF table:

Command	Description
show ip ref route [**default** | {*ip mask*}| **statistics**]	Displays route information in the IPv4 REF table. The parameter **default** indicates a default route.

show ipv6 ref route [**default** | **statistics** | *prefix/len*]	Displays route information in the IPv6 REF table. The parameter **default** indicates a default route.

IP Routing Configuration

1 Configuring RIP

2 Configuring OSPFv2

3 Configuring RIPng

4 Managing Routes

1 Configuring RIP

1.1 Overview

Routing Information Protocol (RIP) is a unicast routing protocol applied on IPv4 networks. RIP-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIP can run only within the autonomous system (AS) and is applicable to small-sized networks whose longest path involves less than 16 hops.

Protocols and Standards

- RFC1058: Defines RIPv1.
- RFC2453: Defines RIPv2.

Note:

"Router" in this chapter refers to the network device that supports the routing function. These network devices can be Layer 3 switches, routers, firewalls, etc.

1.2 Applications

Application	Description
Basic RIP Application	The routing information is automatically maintained through RIP on a small-sized network.

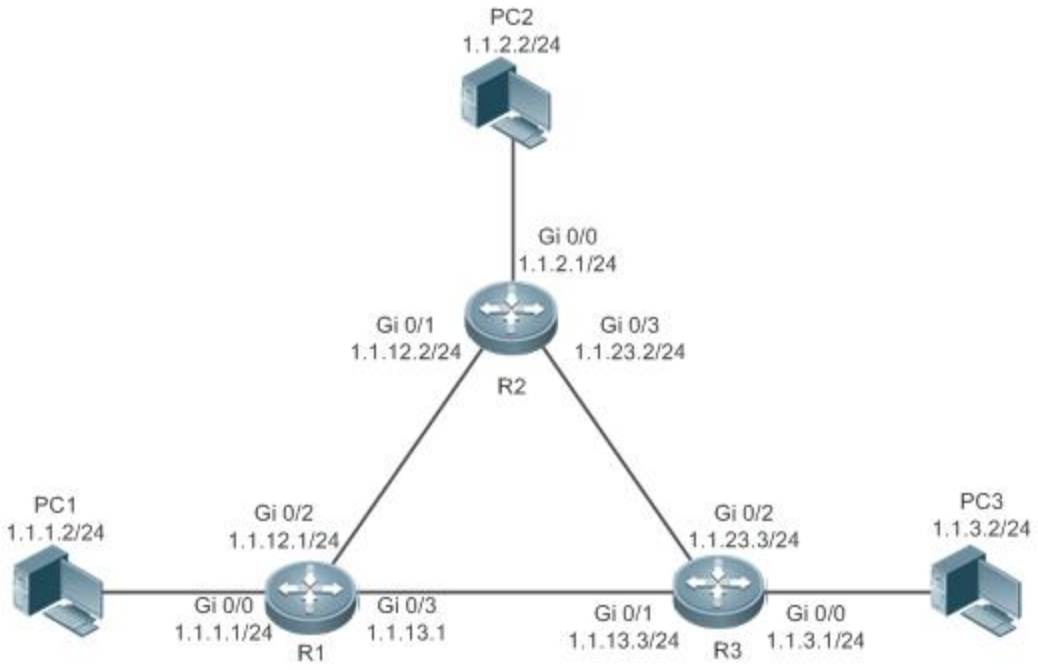
1.2.1 Basic RIP Application

Scenario

On a network with a simple structure, you can configure RIP to implement network interworking. Configuring RIP is simpler than configuring other IGP protocols like Open Shortest Path First (OSPF). Compared with static routes, RIP can dynamically adapt to the network structure changes and is easier to maintain.

As shown in Figure 1-1, to implement interworking between PC1, PC2, and PC3, you can configure RIP routes on R1, R2, and R3.

Figure 1-1



Deployment

- Configure IP addresses and gateways on three PCs.
- Configure IP addresses and subnet masks on three routers.
- Configure RIP on three routers.

1.3 Features

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.

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.

Overview

Feature	Description
RIPv1 and RIPv2	RIP is available in two versions: RIPv1 and RIPv2.
Exchanging Routing Information	By exchanging routing information, RIP-enabled devices can automatically obtain routes to a remote network and update the routes in real time.
Routing Algorithm	RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.
Avoiding Route Loops	RIP uses functions, such as split horizon and poison reverse, to avoid route loops.
Security Measures	RIP uses functions, such as authentication and source address verification, to ensure protocol security.
Reliability Measures	RIP uses functions, such as bidirectional forwarding detection (BFD) correlation, fast reroute, and graceful restart (GR), to enhance reliability of the protocol.

1.3.1 RIPv1 and RIPv2

Two RIP versions are available: RIPv1 and RIPv2.

Working Principle

RIPv1

RIPv1 packets are broadcast. The broadcast address is 255.255.255.255, and the UDP port ID is 520. RIPv1 cannot identify the subnet mask, and supports only classful routes.

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.

Related Configuration

Enabling the RIP Process

The RIP process is disabled by default.

Run the **router rip** command to enable the RIP process.

You must enable the RIP process on a device; otherwise, all functions related to RIP cannot take effect.

Running RIP on an Interface

By default, RIP does not run on an interface.

Run the **network** command to define an address range. RIP runs on interfaces that belong to this address range.

After RIP runs on an interface, RIP packets can be exchanged on the interface and RIP can learn routes to the network segments directly connected to the device.

Defining the RIP Version

By default, an interface receives RIPv1 and RIPv2 packets, and sends RIPv1 packets.

Run the **version** command to define the version of RIP packets sent or received on all interfaces.

Run the **ip rip send version** command to define the version of RIP packets sent on an interface.

Run the **ip rip receive version** command to define the version of RIP packets received on an interface.

⚠ If the versions of RIP running on adjacent routers are different, the RIPv1-enabled router will learn incorrect routes.

Preventing an Interface from Sending or Receiving Packets

By default, a RIP-enabled interface is allowed to send and receive RIP packets.

Run the **no ip rip receive enable** command to prevent an interface from receiving RIP packets.

Run the **no ip rip send enable** command to prevent an interface from sending RIP packets.

Run the **passive-interface** command to prevent an interface from sending broadcast or multicast RIP packets.

Configuring the Mode for Sending RIP Packets

By default, broadcast RIPv1 packets and multicast RIPv2 are sent.

Run the **ip rip v2-broadcast** command to send broadcast RIPv2 packets on an interface.

Run the **neighbor** command to send unicast RIP packets to a specified neighbor router.

1.3.2 Exchanging Routing Information

Compared with static routing, the dynamic routing protocol has a significant advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

Working Principle

Initialization

After RIP is enabled on a router, the router sends a request packet to its neighbor router, requesting for all routing information, that is, the routing table. After receiving the request message, the neighbor router 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 a series of updates, all routers can obtain and retain the latest routing information.

Periodical Update

By default, periodical update is enabled for RIP. Adjacent routers exchange complete routing information with each other every 30s (update timer), that is, the entire routing table is sent to neighbor routers. 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.

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 Updates

After the triggered updates function is enabled, periodical update is automatically disabled. When routing information changes on a router, the router immediately sends routes related to the change (instead of the complete routing table) to the neighbor router, and use the acknowledgment and retransmission mechanisms to ensure that the neighbor router receives the routes successfully. Compared with periodical update, triggered updates help 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 router, the RIP-enabled router summarizes subnet routes that belong to the same classful network into a route, and sends the route to the neighbor router. 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), and set the metric of the summarized route to the optimum metric.

Only RIPv2 supports route summarization. Route summarization can reduce the size of the routing table and improve the efficiency of routing information exchange.

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, in the 80.0.0.0/6 route, 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.

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 router, or sent to a neighbor router.

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.

Related Configuration

Sending Delay Between Update Packets

By default, the update packets are sent continuously without any delay.
Run the **output-delay** command to set the sending delay between update packets.

RIP Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Run the **timers basic** command to modify durations of the RIP timers.

Increasing the duration of the flush timer can reduce the route flapping. Decreasing the duration of the flush timer helps accelerate route convergence.

The durations of RIP timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to modify the RIP timers.

Triggered Updates

By default, periodical update is enabled.

Run the **ip rip triggered** command to enable triggered updates on the interface and disable periodical update.

Run the **ip rip triggered retransmit-timer** command to modify the retransmission interval of update packets. The default value is 5s.

Run the **ip rip triggered retransmit-count** command to modify the maximum retransmission times of update packets. The default value is 36.

Route Summarization

By default, route summarization is automatically enabled if an interface is allowed to send RIPv2 packets.

Run the **no auto-summary** command to disable route summarization.

Run the **ip rip summary-address** command to configure route summarization on an interface.

Supernetting Route

By default, supernetting routes can be sent if an interface is allowed to send RIPv2 packets.

Run the **no ip rip send supernet-routes** command to prevent the sending of supernetting routes.

Default Route

Run the **ip rip default-information** command to advertise the default route to neighbors on an interface.

Run the **default-information originate** command to advertise the default route to neighbors from all interfaces.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIP and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit the routing information sent by the device.

Run the **distribute-list in** command to set filtering rules to limit the routing information received by the device.

1.3.3 Routing Algorithm

RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

Working Principle

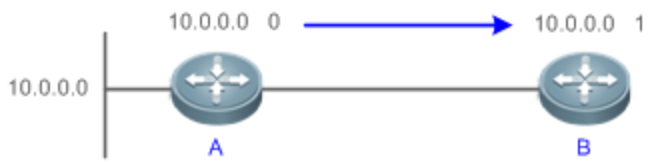
Distance-Vector Algorithm

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 (metric). 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.

RIP uses the hop count to evaluate the distance (metric) 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 the 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, RIP stipulates that the metric must be an integer between 0 and 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 on a large-scale network.

As shown in Figure 1-2, Router A is connected to the network 10.0.0.0. Router B obtains the route (10.0.0.0,0) from Router 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 Router A.

Figure 1-2

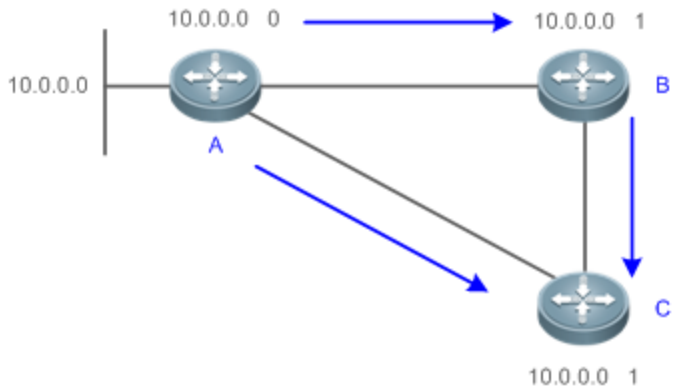


Selecting the Optimum Route

RIP selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a router preferentially selects the route with the smallest metric.

As shown in Figure 1-3, Router A is connected to the network 10.0.0.0. Router C obtains the route (10.0.0.0,0) from Router A and the route (10.0.0.0,1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (10.0.0.0,1), and the next hop points to Router A.

Figure 1-3



When routes coming from different sources exist on a router, the route with the smallest distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
RIP route	120
Unreachable route	255

Related Configuration

Modifying the Distance

By default, the distance of a RIP route is 120.

Run the **distance** command to modify the distance of a RIP route.

Modifying the Metric

For a RIP route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. For a RIP router that is manually configured (default route or redistributed route), the default metric is 1.

Run the **offset-list in** command to increase the metric of a received RIP route.

Run the **offset-list out** command to increase the metric of a sent RIP route.

Run the **default-metric** command to modify the default metric of a redistributed route.

Run the **redistribute** command to modify the metric of a route when the route is redistributed.

Run the **default-information originate** command to modify the metric of a default route when the default route is introduced.

Run the **ip rip default-information** command to modify the metric of a default route when the default route is created.

1.3.4 Avoiding Route Loops

RIP uses functions, such as split horizon and poison reverse, to avoid route loops.

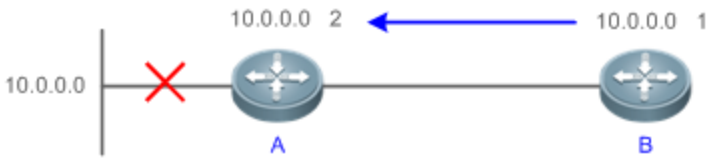
Working Principle

Route Loop

A RIP route loop occurs due to inherent defects of the distance-vector algorithm.

As shown in Figure 1-4, Router A is connected to the network 10.0.0.0, and sends an update packet every 30s. Router B receives the route 10.0.0.0 from Router A every 30s. If Router A is disconnected from 10.0.0.0, the route to 10.0.0.0 will be deleted from the routing table on Router A. Next time, the update packet sent by Router A no longer contains this route. As Router B does not receive an update packet related to 10.0.0.0, Router B determines that the route to 10.0.0.0 is valid within 180s and uses the Update packet to send this route to Router A. As the route to 10.0.0.0 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 10.0.0.0 through Router A, and Router A determines that data can reach 10.0.0.0 through Router B. In this way, a route loop is formed.

Figure 1-4



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 1-5, after split horizon is enabled on the interface between Router A and Router B, Router B will not send the route 10.0.0.0 back to Router A. Router B will learn 180s later that 10.0.0.0 is not reachable.

Figure 1-5



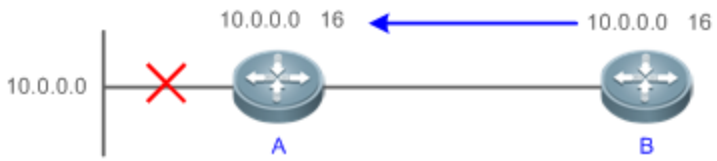
Poison Reverse

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 1-6, after learning the route 10.0.0.0 from Router A, Router B sets the metric of this route to 16 and sends the route back to Router A. After this route becomes invalid, Router B advertises the route 10.0.0.0 (metric = 16) to Router A to accelerate the process of deleting the route from the routing table.

Figure 1-6



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no ip rip split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **ip rip split-horizon poisoned-reverse** command to enable poison reverse. (After poison reverse is enabled, split horizon is automatically disabled.)

1.3.5 Security Measures

RIP uses functions, such as authentication and source address verification, to ensure protocol security.

Working Principle

Authentication

RIPv2 supports authentication, but RIPv1 does not.

After authentication is enabled on an interface, the routing information cannot be exchanged between adjacent devices if authentication fails. The authentication function is used to prevent unauthorized devices from accessing the RIP routing domain.

RIPv2 supports plain text authentication and MD5 authentication.

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.

- 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).

Related Configuration

Authentication

By default, authentication is disabled.

Run the **ip rip authentication mode text** command to enable plain text authentication on an interface.

Run the **ip rip authentication mode md5** command to enable MD5 authentication on an interface.

Run the **ip rip authentication text-password** command to set the password for plain text authentication on an interface.

Run the **ip rip authentication key-chain** command to reference the key in the configured key chain as the authentication key on an interface.

Source Address Verification

By default, source address verification is enabled.

Run the **no validate-update-source** command to disable source address verification.

1.3.6 Reliability Measures

RIP uses functions and GR, to enhance reliability of the protocol.

Working Principle

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.

Related Configuration

GR

By default, GR is disabled.

Run the **graceful-restart** command to enable the GR function.

1.4 Configuration

Configuration	Description and Command
Configuring RIP Basic	(Mandatory) It is used to build a RIP routing domain.

Configuration	Description and Command	
Functions	**router rip**	Enables a RIP routing process and enters routing process configuration mode.
	network	Runs RIP on interfaces in the specified address range.
	version	Defines the RIP version.
	ip rip split-horizon	Enables split horizon or poison reverse on an interface.
	passive-interface	Configures a passive interface.
Controlling Interaction of RIP Packets	(Optional) This configuration is required if you wish to change the default mechanism for sending or receiving RIP packets.	
	neighbor	Sends unicast RIP packets to a specified neighbor.
	ip rip v2-broadcast	Sends broadcast RIPv2 packets on an interface.
	ip rip receive enable	Allows the interface to receive RIP packets.
	ip rip send enable	Allows the interface to send RIP packets.
	ip rip send version	Defines the version of RIP packets sent on an interface.
	ip rip receive version	Defines the version of RIP packets received on an interface.
Enabling Triggered Updates	Optional.	
	ip rip triggered	Enables triggered updates on an interface.
Enabling Source Address Verification	Optional.	
	validate-update-source	Enables source address verification.
Enabling Authentication	(Optional) Only RIPv2 supports authentication.	
	ip rip authentication mode	Enables authentication and sets the authentication mode on an interface.
	ip rip authentication text-password	Configures the password for plain text authentication on an interface.
	ip rip authentication key-chain	Configures the authentication key chain on an interface.
Enabling Route Summarization	(Optional) Only RIPv2 supports route summarization.	
	auto-summary	Enables automatic summarization of RIP routes.
	ip rip summary-address	Configures route summarization on an interface.
Enabling Supernetting Routes	(Optional) Only RIPv2 supports supernetting routes.	
	ip rip send supernet-routes	Enables advertisement of RIP supernetting

Configuration	Description and Command	
		routes on an interface
Advertising the Default Route or External Routes	⚠ Optional.	
	ip rip default-information	Advertises the default route to neighbors on an interface.
	default-information originate	Advertises the default route to neighbors.
	redistribute	Redistributes routes and advertises external routes to neighbors.
Setting Route Filtering Rules	⚠ Optional.	
	distribute-list in	Filters the received RIP routing information.
	distribute-list out	Filters the sent RIP routing information.
Modifying Route Selection Parameters	⚠ Optional.	
	distance	Modifies the administrative distance (AD) of a RIP route.
	offset-list	Increases the metric of a received or sent RIP route.
	default-metric	Configures the default metric of an external route redistributed to RIP.
Modifying Timers	⚠ Optional.	
	timers basic	Modifies the update timer, invalid timer, and flush timer.
	output-delay	Sets the sending delay between RIP route update packets.
Enabling GR	⚠ Optional.	
	graceful-restart	Configures the GR restarter capability.

1.4.1 Configuring RIP Basic Functions

Configuration Effect

- Build a RIP routing domain on the network.
- Routers in the domain obtain routes to a remote network through RIP.

Notes

- IPv4 addresses must be configured.
- IPv4 unicast routes must be enabled.

Configuration Steps

↘ **Enabling a RIP Routing Process**

- Mandatory.
- Unless otherwise required, this configuration must be performed on every router in the RIP routing domain.

Associating with the Local Network

- Mandatory.
- Unless otherwise required, this configuration must be performed on every router in the RIP routing domain.
- Unless otherwise required, the local network associated with RIP should cover network segments of all L3 interfaces.

Defining the RIP Version

- If RIPv2 functions (such as the variable length subnet mask and authentication) are required, enable the RIPv2.
- Unless otherwise required, you must define the same RIP version on every router.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on every interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on every interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected to a non-broadcast multi-access (NBMA) network, such as FR and X.25; otherwise, some devices may fail to learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- If you want to suppress Update packets on a RIP interface, configure the interface as a passive interface.
- Use the passive interface to set the boundary of the RIP routing domain. The network segment of the passive interface belongs to the RIP routing domain, but RIP packets cannot sent over the passive interface.
- If RIP routes need to be exchanged on an interface (such as the router interconnect interface) in the RIP routing domain, this interface cannot be configured as a passive interface.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIP.

Related Commands

Enabling a RIP Routing Process

Command	router rip

Syntax	
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to create a RIP routing process and enter routing process configuration mode.

Associating with the Local Network

Command Syntax	**network** *network-number* [*wildcard*]
Parameter Description	*network-number*: Indicates the number of a network. *wildcard*: Defines the IP address comparison bit. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	RIP can run and learn direct routes and RIP packets can be exchanged only on an interface covered by **network**. If **network** 0.0.0.0 255.255.255.255 is configured, all interfaces are covered. If *wildcard* 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.

Defining the RIP Version

Command Syntax	**version** { **1** | **2** }
Parameter Description	**1**: Indicates RIPv1. **2**: Indicates RIPv2.
Command Mode	Global configuration mode
Configuration Usage	This command takes effect on the entire router. You can run this command to define the version of RIP packets sent or received on all interfaces.

Enabling Split Horizon

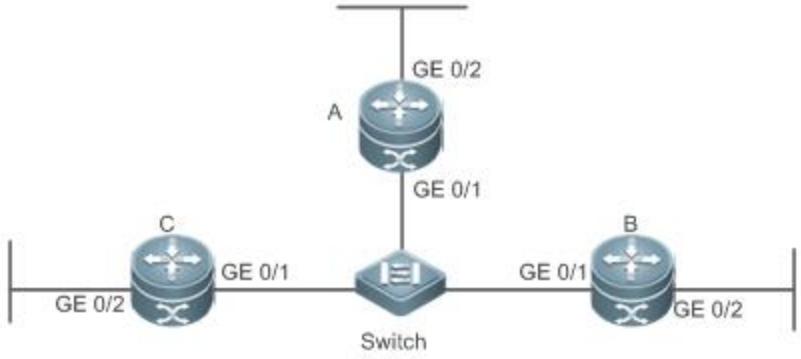
Command Syntax	**ip rip split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates poison reverse.
Command Mode	Interface configuration mode
Configuration Usage	After poison reverse is enabled, split horizon is automatically disabled.

Configuring a Passive Interface

Command Syntax	**passive-interface** { **default** | *interface-type interface-num* }
Parameter Description	**default:** Indicates all interfaces. ***interface-type interface-num*:** Specifies an interface.
Command Mode	Routing process configuration mode
Configuration Usage	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command to cancel the interfaces used for interconnection between routers in the domain.

Configuration Example

Building a RIP Routing Domain

Scenario **Figure 1-7**	 **Remarks** The interface IP addresses are as follows: A: GE0/1 110.11.2.1/24 GE0/2 155.10.1.1/24 B: GE0/1 110.11.2.2/24 GE0/2 196.38.165.1/24 C: GE0/1 110.11.2.3/24 GE0/2 117.102.0.1/16
Configuration Steps	● Configure the interface IP addresses on all routers. ● Configure the RIP basic functions on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0 A(config)# router rip A(config-router)# version 2 A(config-router)# network 0.0.0.0 255.255.255.255

	A(config-router)# passive-interface default A(config-router)# no passive-interface GigabitEthernet 0/1
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router rip B(config-router)# version 2 B(config-router)# network 0.0.0.0 255.255.255.255 B(config-router)# passive-interface default B(config-router)# no passive-interface GigabitEthernet 0/1
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# router rip C(config-router)# version 2 C(config-router)#no auto-summary C(config-router)# network 0.0.0.0 255.255.255.255 C(config-router)# passive-interface default C(config-router)# no passive-interface GigabitEthernet 0/1
Verification	Check the routing tables on Router A, Router B, and Router C. Verify that RIP learns the routes to remote networks (contents marked in blue).
A	A# show ip route

	Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1 C 155.10.1.0/24 is directly connected, GigabitEthernet 0/2 C 155.10.1.1/32 is local host. C 192.168.217.0/24 is directly connected, VLAN 1 C 192.168.217.233/32 is local host. R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
B	B# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.2/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1 C 196.38.165.0/24 is directly connected, GigabitEthernet 0/2

	C 196.38.165.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C	C# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.3/32 is local host. C 117.102.0.0/16 is directly connected, GigabitEthernet 0/2 C 117.102.0.1/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1 R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1 This series does not support ISIS or BGP. The configuration example is only for reference.

Common Errors

- The IPv4 address is not configured on an interface.
- The RIP version is not defined on a device, or the RIP version on the device is different from that on other routers.
- The address range configured by the **network** command does not cover a specific interface.
- The **wildcard** parameter in the **network** command is not correctly configured. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
- The interface used for interconnection between devices is configured as a passive interface.

1.4.2 Controlling Interaction of RIP Packets

Configuration Effect

Change the default running mechanism of RIP through configuration and manually control the interaction mode of RIP packets, including:

- 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

Notes

- The RIP basic functions 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.

Configuration Steps

Sending Unicast RIP Route Update Packets to a Specified Neighbor

- Configure this function if you wish that only some of devices connected to an interface can receive the up dated routing information.
- By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise the routing information, whereas RIPv2 uses the multicast address (224.0.0.9) to advertise the routing information. If you do not wish all devices on the broadcast network or NBMA network to receive routing information, configure the related interface as the passive interface and specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. RIPv2 packets are broadcast on an interface.
- Unless otherwise required, this function must be enabled on a router that sends the unicast Update packets.

Broadcasting RIPv2 Packets on an Interface

- This function must be configured if the neighbor router does not support the receiving of multicast RIPv2 packets.
- Unless otherwise required, this function must be configured on every router interface that broadcasts RIPv2 packets.

Allowing an Interface to Receive RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to receive RIP packets.
- Unless otherwise required, this function must be configured on every router interface that is not allowed to receive RIP packets.

Allowing an Interface to Send RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to send RIP packets.
- Unless otherwise required, this function must be configured on every router interface that is not allowed to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be sent on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on every router interface that is allowed to send RIP packets of a specified version.

Allowing an Interface to Receive RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be received on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on every router interface that is allowed to receive RIP packets of a specified version.

Verification

Run the **debug ip rip packet** command to verify the packet sending result and packet type.

Related Commands

Sending Unicast RIP Route Update Packets to a Specified Neighbor

Command Syntax	**neighbor** *ip-address*
Parameter Description	*ip-address:* Indicates the IP address of the neighbor. It should be the address of the network directly connected to the local device.
Command Mode	Routing process configuration mode
Configuration Usage	Generally, you can first run the **passive-interface** command in routing process configuration mode to configure the related interface as a passive interface, 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 the request packets even after the device is restarted.

Broadcasting RIPv2 Packets on an Interface

Command Syntax	**ip rip v2-broadcast**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by 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 is determined by the configuration of the **version** command.

Allowing an Interface to Receive RIP Packets

Command Syntax	**ip rip receive enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	To prohibit the receiving of RIP packets on an interface, use the **no** form of this command. This command takes effect only on the current interface. You can use the **default** form of the command to restore the default setting, that is, allowing the interface to receive RIP packets.

Allowing an Interface to Send RIP Packets

Command Syntax	**ip rip send enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	To prohibit the sending of RIP packets on an interface, use the **no** form of this command in interface configuration mode. This command takes effect only on the current interface. You can use the **default** form of the command to restore the default setting, that is, allowing the interface to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

Command Syntax	**ip rip send version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are sent. **2**: Indicates that only RIPv2 packets are sent.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by 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 is determined by the configuration of the **version** command.

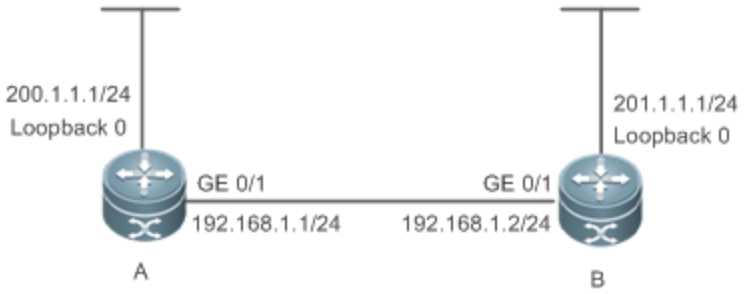
Allowing an Interface to Receive RIP Packets of a Specified Version

Command Syntax	**ip rip receive version** [**1**] [**2**]

Parameter Description	**1**: Indicates that only RIPv1 packets are received. **2**: Indicates that only RIPv2 packets are received.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by 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 is determined by the configuration of the **version** command.

Configuration Example

↘ Prohibiting an Interface from Sending RIP Packets

Scenario **Figure 1-8**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Prohibit the sending of RIP packets on an interface of Router A.

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# no ip rip send enable`

Verification	Run the **debug ip rip packet send** command on Router A, and verify that packets cannot be sent.

A	`A# debug ip rip packet recv`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Prepare to send BROADCAST response...`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Building update entries on GigabitEthernet 0/1`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: 117.0.0.0/8 via 0.0.0.0 metric 1 tag 0`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Interface GigabitEthernet 0/1 is disabled to send RIP packet!`

Common Errors

A compatibility error occurs because the RIP version configured on the neighbor is different from that configured on the local device.

1.4.3 Enabling Triggered Updates

Configuration Effect

- Enable the RIP triggered updates function, after which RIP does not periodically send the route update packets.

Notes

- The RIP basic functions must be configured.
- It is recommended that split horizon with poisoned reverse be enabled; otherwise, invalid routing information may exist.
- Ensure that the triggered updates function is enabled on every router on the same link; otherwise, the routing information cannot be exchanged properly.

Configuration Steps

↘ Enabling Triggered Updates

- This function must be enabled if demand circuits are configured on the WAN interface.
- The triggered updates function can be enabled in either of the following cases: (1) The interface has only one neighbor; (2) The interface has multiple neighbors but the device interacts with these neighbors in unicast mode.
- It is recommended that triggered updates be enabled on a WAN interface (running the PPP, Frame Relay, or X.25 link layer protocol) to meet the requirements of demand circuits.
- If the triggered updates function is enabled on an interface, source address verification is performed no matter whether the source address verification function is enabled by the **validate-update-source** command.
- Unless otherwise required, triggered updates must be enabled on demand circuits of every router.

Verification

When the RIP triggered updates function is enabled, RIP cannot periodically send the route update packets. RIP sends the route update packets to the WAN interface only in one of the following cases:

- A route request packet is received.
- The RIP routing information changes.
- The interface state changes.
- The router is started.

Related Commands

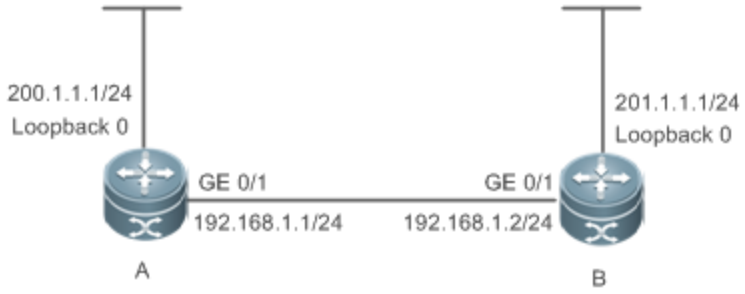
↘ Enabling Triggered Updates

Command Syntax	**ip rip triggered** { **retransmit-timer** *timer* | **retransmit-count** *count* }
Parameter Description	**retransmit-timer** *timer*: Configures the interval at which the update request or update response packet is retransmitted. The default value is 5s. The value ranges from 1 to 3,600. **retransmit-count** *count*: Configures the maximum retransmission times of the update request or update

	response packet. The default value is 36. The value ranges from 1 to 3,600.
Command Mode	Interface configuration mode
Configuration Usage	You can run the **ip rip triggered** command to enable the RIP triggering function. When this function is enabled, the RIP periodical update function is automatically disabled. Therefore, the acknowledgment and retransmission mechanisms must be used to ensure that the Update packets are successfully sent or received on the WAN. You can use the **retransmit-timer** and **retransmit-count** parameters to specify the retransmission interval and maximum retransmission times of the request and update packets.

Configuration Example

↘ Enabling Triggered Updates

Scenario Figure 1-9	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router A, enable the RIP triggered updates function, and set the retransmission interval and maximum retransmission times of the request and update packets to 10s and 18, respectively.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# encapsulation ppp A(config-if-GigabitEthernet 0/1)# ip rip triggered A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10 A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18 A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse A(config)# router rip A(config-router)# network 192.168.1.0 A(config-router)# network 200.1.1.0
B	B# configure terminal

	B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# encapsulation ppp B(config-if-GigabitEthernet 0/1)# ip rip triggered B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse B(config)# router rip B(config-router)# network 192.168.1.0 B(config-router)# network 201.1.1.0
Verification	On Router A and Router B, check the RIP database and verify that the corresponding routes are permanent.
A	A# sho ip rip database 201.1.1.0/24 auto-summary 201.1.1.0/24 [1] via 192.168.12.2 GigabitEthernet 0/1 06:25 permanent
B	B# sho ip rip database 200.1.1.0/24 auto-summary 200.1.1.0/24 [1] via 192.168.12.1 GigabitEthernet 0/1 06:25 permanent

Common Errors

- The triggered updates function is enabled when the RIP configurations at both ends of the link are consistent.
- The triggered updates function is not enabled on all routers on the same link.

1.4.4 Enabling Source Address Verification

Configuration Effect

- The source address of the received RIP route update packet is verified.

Notes

- The RIP basic functions must be configured.

Configuration Steps

↘ Enabling Source Address Verification

- This function is enabled by default, and must be disabled when source address verification is not required.

- After split horizon is disabled on an interface, the RIP routing process will perform source address verification on the Update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- For an IP unnumbered interface, the RIP routing process does not perform source address verification on the Update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- Unless otherwise required, this function must be disabled on every router that does not requires source address verification.

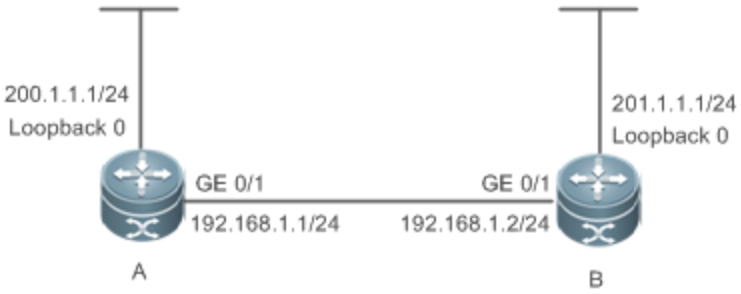
Verification

Only the route update packets coming from the same IP subnet neighbor are received.

Related Commands

Command Syntax	**validate-update-source**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Source address verification of the Update packet is enabled by default. After this function is enabled, the source address of the RIP route update packet is verified. The purpose is to ensure that the RIP routing process receives only the route update packets coming from the same IP subnet neighbor.

Configuration Example

Scenario Figure 1-10	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Disable source address verification of Update packets on all routers.

A	`A# configure terminal`
	`A(config)# router rip`
	`A(config-router)# no validate-update-source`

B	B# configure terminal B(config)# router rip B(config-router)# no validate-update-source
Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.2.2, 00:06:11, GigabitEthernet 0/1
B	B# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

1.4.5 Enabling Authentication

Configuration Effect

- Prevent learning unauthenticated and invalid routes and advertising valid routes to unauthorized devices, ensuring stability of the system and protecting the system against intrusions.

Notes

- The RIP basic functions must be configured.
- Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

Configuration Steps

↘ Enabling Authentication and Specifying the Key Chain Used for RIP Authentication

- This configuration is mandatory if authentication must be enabled.
- If the key chain is already specified in the interface configuration, run the **key chain** command in global configuration mode to define the key chain; otherwise, authentication of RIP packets may fail.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

↘ Defining the RIP Authentication Mode

- This configuration is mandatory if authentication must be enabled.
- The RIP authentication modes configured on all devices that need to directly exchange RIP routing information must be the same; otherwise, RIP packets may fail to be exchanged.
- If plain text authentication is used, but the key chain for plain text authentication is not configured or associated, authentication is not performed. Similarly, if MD5 authentication is used, but the key chain is not configured or associated, authentication is not performed.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Enabling RIP Plain Text Authentication and Configuring the Key Chain

- This configuration is mandatory if authentication must be enabled.
- If RIP plain text authentication should be enabled, use this command to configure the key chain for plain text authentication. Alternatively, you can obtain the key chain for plain text authentication by associating the key chain. The key chain obtained using the second method takes precedence over that obtained using the first method.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Verification

- RIP plain text authentication provides only limited security because the password transferred through the packet is visible.
- RIP MD5 authentication can provide higher security because the password transferred through the packet is encrypted using the MD5 algorithm.
- Routes can be learned properly if the correct authentication parameters are configured.
- Routes cannot be learned if the incorrect authentication parameters are configured.

Related Commands

Enabling Source Address Verification

Command Syntax	**ip rip authentication key-chain** *name-of-keychain*
Parameter Description	*name-of-keychain*: Specifies the name of the key chain used for RIP authentication.
Command Mode	Interface configuration mode
Configuration Usage	The specified key chain must be defined by the **key chain** command in global configuration mode in advance.

Defining the RIP Authentication Mode

Command Syntax	**ip rip authentication mode** { **text** | **md5** }
Parameter Description	**text:** Indicates that the RIP authentication mode is plain text authentication. **md5:** Indicates that the RIP authentication mode is MD5 authentication.
Command Mode	Interface configuration mode
Configuration Usage	For all devices that need to directly exchange the RIP routing information, the RIP authentication mode of these devices must be the same.

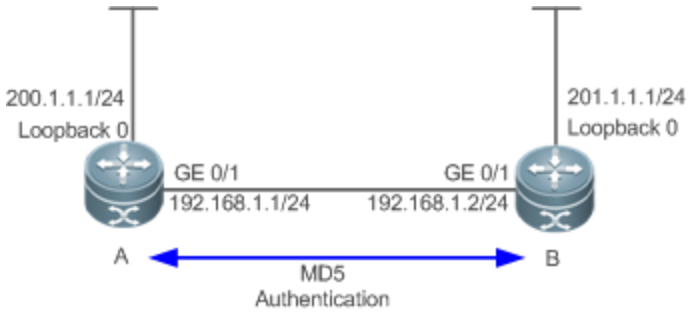
Enabling RIP Plain Text Authentication and Configuring the Key Chain

Command	**ip rip authentication text-password** [**0** | **7**] *password-string*

Syntax	
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *password-string*: Indicates the key chain used for plain text authentication. The key chain is a string of 1 to 16 bytes.
Command Mode	Interface configuration mode
Configuration Usage	This commands takes effect only in plain text authentication mode.

Configuration Example

Configuring RIP Basic Functions and Enabling MD5 Authentication

Scenario Figure 1-11	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.

A	`A# configure terminal`
	`A(config)# key chain hello`
	`A(config-keychain)# key 1`
	`A(config-keychain-key)# key-string world`
	`A(config-keychain-key)# exit`
	`A(config-keychain)# exit`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5`
	`A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello`

B	`B# configure terminal`
	`B(config)# key chain hello`
	`B(config-keychain)# key 1`
	`B(config-keychain-key)# key-string world`

	B(config-keychain-key)# exit B(config-keychain)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
Verification	• On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. • On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

Common Errors

- The keys configured on routers that need to exchange RIP routing information are different.
- The authentication modes configured on routers that need to exchange RIP routing information are different.

1.4.6 Enabling Route Summarization

Configuration Effect

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.

- If a summarized route exists, subroutes included by the summarized route cannot be seen in the routing table, which greatly reduces the size of the routing table.
- Advertising a summarized route is more efficient than advertising individual routes because: (1) A summarized route is processed first when RIP looks through the database; (2) All subroutes are ignored when RIP looks through the database, which reduces the processing time required.

Notes

- The RIP basic functions 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 always performs automatic route summarization. If the detailed routes should be advertised, you must set the RIP version to RIPv2.

Configuration Steps

Enabling Automatic Route Summarization

- This function is enabled by default.
- To learn specific subnet routes instead of summarized network routes, you must disable automatic route summarization.
- You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

- This function must be configured if it is required to summarize classful subnets.
- The **ip rip summary-address** command is used to summarize an address or a subnet under a specified interface. RIP automatically summarizes to the classful network boundary. Each classful subnet can be configured only in the **ip rip summary-address** command.
- The summary range configured in this command cannot be supernetting routes, that is, the configured subnet mask length cannot be smaller than the natural mask length of the network.
- Unless otherwise required, this configuration should be performed on a router that requires classful subnet summarization.

Verification

Verify that the routes are summarized in the routing table of the peer end.

Related Commands

Enabling Automatic Route Summarization

Command Syntax	**auto-summary**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Route summarization is enabled by default for RIPv1 and RIPv2. You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

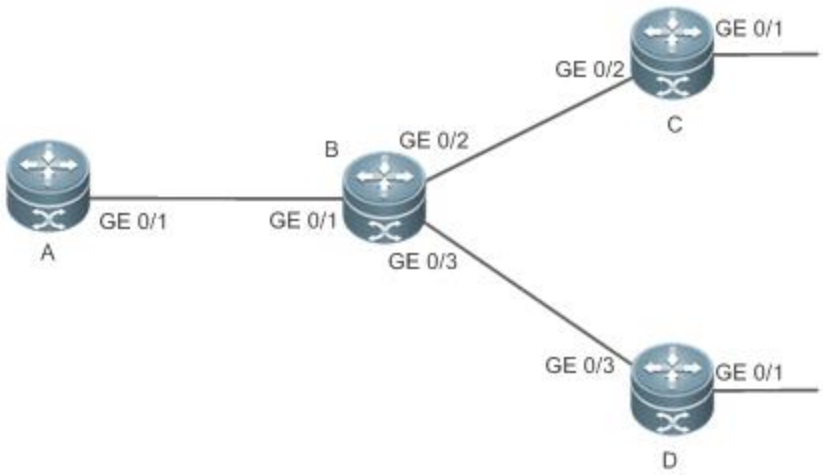
Configuring RIP Route Summarization on an Interface

Command Syntax	**ip rip summary-address** *ip-address ip-network-mask*
Parameter Description	*ip-address*: Indicates the IP address to be summarized. *ip-network-mask*: Indicates the subnet mask of the IP address to be summarized.
Command Mode	Interface configuration mode

Configuration Usage	This command is used to summarize an address or a subnet under a specified interface.

Configuration Example

↘ Configuring Route Summarization

Scenario Figure 1-12	 **Remarks** The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure route summarization on Router B.
	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0 B(config)# router rip B(config-router)# version 2 B(config-router)# no auto-summary
Verification	Check the routing table on Router A, and verify that the entry 172.16.0.0/16 is generated.
	A# show ip route rip R 172.16.0.0/16 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

Common Errors

- RIP basic functions are not configured or fail to be configured.

1.4.7 Enabling Supernetting Routes

Configuration Effect

- Allow RIP to send RIP supernetting routes on a specified interface.

Notes

- The RIP basic functions must be configured.

Configuration Steps

↘ **Enabling Supernetting Routes**

- If a supernetting route is detected when a RIPv1-enabled router monitors the RIPv2 route response packets, the router will learn an incorrect route because RIPv1 ignores the subnet mask in the routing information of the packet. In this case, the **no** form of the command must be used on the RIPv2-enabled router to prohibit advertisement of supernetting routes on the related interface. This command takes effect only on the current interface.
- The command is effective only when RIPv2 packets are sent on the interface, and is used to control the sending of supernetting routes.

Verification

Verify that the peer router cannot learn the supernetting route.

Related Commands

Command Syntax	**ip rip send supernet-routes**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	By default, an interface is allowed to send RIP supernetting routes.

Configuration Example

↘ **Disabling Supernetting Routes**

Scenario **Figure 1-13**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Prohibit the sending of RIP supernetting routes on the GigabitEthernet 0/1 interface of Router B.
	B# configure terminal B(config)# ip route 207.0.0.0 255.0.0.0 Null 0 B(config)# ip route 208.1.1.0 255.255.255.0 Null 0 B(config)# router rip B(config-router)# redistribute static B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes
Verification	Check the routing table on Router A, and verify that Router A can learn only the non-supernetting route 208.1.1.0/24, but not the supernetting route 207.0.0.0/8.
	A#show ip route rip R 208.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

1.4.8 Advertising the Default Route or External Routes

Configuration Effect

- In the RIP domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.
- In the RIP domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

Notes

- The RIP basic functions must be configured.
- Route redistribution cannot introduce default routes of other protocols to the RIP routing domain.

Configuration Steps

↘ Advertising the Default Route to Neighbors

This function must be enabled if it is required to advertise the default route to neighbors.

By default, a default route is not generated, and the metric of the default route is 1.

If the RIP process can generate a default route using this command, RIP does not learn the default route advertised by the neighbor.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

Advertising the Default Route to Neighbors on an Interface

This function must be enabled if it is required to advertise the default route to neighbors on a specified interface.

By default, a default route is not configured and the metric of the default route is 1.

After this command is configured on an interface, a default route is generated and advertised through this interface.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

Redistributes Routes and Advertises External Routes to Neighbors

This function must be enabled if routes of other protocols need to be redistributed.

By default,

- If OSPF redistribution is configured, redistribute the routes of all sub-types of the OSPF process.
- In other cases, redistribute all external routes.
- The metric of a redistributed route is 1 by default.
- The route map is not associated by default.

During route redistribution, it is not necessary to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use completely different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other. During route redistribution, however, it is necessary to configure a symbolic metric; otherwise, route redistribution fails.

Unless otherwise required, this configuration should be performed on a router that needs to redistribute routes.

Verification

- On a neighbor device, verify that a default route exists in the RIP routing table.
- On the local and neighbor devices, verify that external routes (routes to other ASs) exist in the RIP routing table.

Related Commands

Advertising the Default Route to Neighbors

Command Syntax	**default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]
Parameter Description	**always:** Enables RIP to generate a default route no matter whether the local router has a default route. **metric** *metric-value:* Indicates the initial metric of the default route. The value ranges from 1 to 15. **route-map** *map-name:* Indicates the associated route map name. By default, no route map is associated.

Command Mode	Routing process configuration mode
Configuration Usage	If a default route exists in the routing table of a router, RIP does not advertise the default route to external entities by default. You need to run the **default-information originate** command in routing process configuration mode to advertise the default route to neighbors. If the **always** parameter is selected, the RIP routing process advertises a default route to neighbors no matter the default route exists, but this default route is not displayed in the local routing table. To check whether the default route is generated, run the **show ip rip database** command to check the RIP routing information database. To further control the behavior of advertising the RIP default route, use the **route-map** parameter. For example, run the **set metric** rule to set the metric of the default route. You can use the **metric** parameter to set the metric of the advertised default value, but the priority of this configuration is lower than that of the set metric rule of the **route-map** parameter. If the **metric** parameter is not configured, the default route uses the default metric configured for RIP. You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

Advertising the Default Route to Neighbors on an Interface

Command Syntax	**ip rip default-information** { **only** | **originate** } [**metric** *metric-value*]
Parameter Description	**only**: Indicates that only the default route is advertised. **originate**: Indicates that the default route and other routes are advertised. **metric** *metric-value:* Indicates the metric of the default route. The value ranges from 1 to 15.
Command Mode	Interface configuration mode
Configuration Usage	If you configure the **ip rip default-information** command for the interface, and the **default-information originate** command for the RIP process, only the default route configured for the interface is advertised. So far as **ip rip default-information** is configured for one interface, RIP does not learn the default route advertised by the neighbor.

Redistributes Routes and Advertises External Routes to Neighbors

Command Syntax	**redistribute** { **connected** | **ospf** *process-id* | **static** } [**metric** *metric-value*] [**route-map** *route-map-name*]
Parameter Description	**connected**: Indicates redistribution from direct routes. **ospf** *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value ranges from 1 to 65535. **static**: Indicates redistribution from static routes. **metric** *metric-value*: Sets the metric of the redistributed route. The value ranges from 1 to 16. **route-map** *route-map-name*: Sets the redistribution filtering rules.
Command Mode	Routing process configuration mode

Configuration Usage	The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

Configuration Example

Redistributing Routes and Advertising External Routes to Neighbors

Scenario **Figure 1-14**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router B, configure redistribution of static routes.

B	`B# configure terminal`
	`B(config)# router rip`
	`B(config-router)# redistribute static`

Verification	On Router A, check the routing table and verify that the entry 172.10.10.0/24 is loaded.
	`A# show ip route rip` `R  172.10.10.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`

1.4.9 Setting Route Filtering Rules

Configuration Effect

- 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.

Notes

- The RIP basic functions must be configured.
- In regard to the filtering rules of sent routes, you must configure route redistribution first, and then filter the redistributed routes.

Configuration Steps

Filtering the Received RIP Routing Information

- This function must be configured if it is required to filter received routing information.
- To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Filtering the Sent RIP Routing Information

- This function must be configured if it is required to filter the redistributed routing information that is sent.
- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route rip** command to verify that the routes that have been filtered out are not loaded to the routing table.

Related Commands

Filtering the Received RIP Routing Information

Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be received. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. **gateway** *prefix-list-name*: Uses the prefix list to filter the route sources. *interface-type interface-number*: Indicates that the distribution list is applied to the specified interface.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

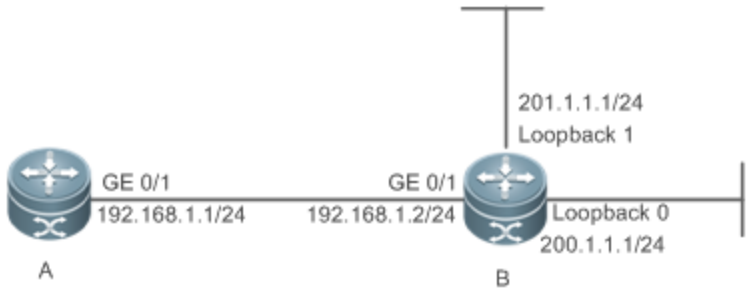
Filtering the Sent RIP Routing Information

Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected**] **| ospf** *process-id* **| rip | static**]]
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be sent. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. *Interface*: Applies route update advertisement control only on the specified interface. **connected**: Applies route update advertisement control only on direct routes introduced through redistribution.

	ospf *process-id*: Applies route update advertisement control only on the routes introduced from OSPF. *process-id* specifies an OSPF process. **rip**: Applies route update advertisement control only on RIP routes. **static**: Applies route update advertisement control only on static routes introduced through redistribution.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

Configuration Example

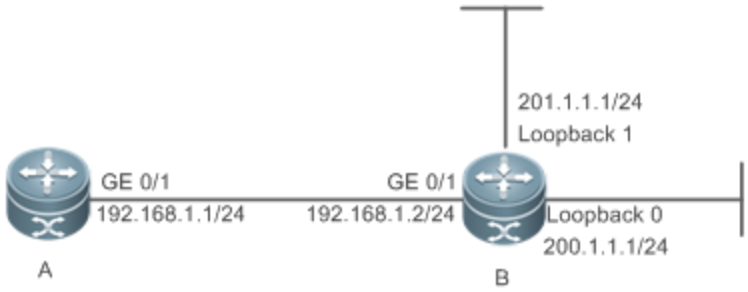
Filtering the Received RIP Routing Information

Scenario Figure 1-15	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Enable the RIP routing process to control routes received over the GigabitEthernet 0/1 port and receive only the route 200.1.1.0.

A	`A# configure terminal`
	`A(config)# router rip`
	`A(config-router)# distribute-list 10 in GigabitEthernet 0/1`
	`A(config-router)# no auto-summary`
	`A(config)# access-list 10 permit 200.1.1.0 0.0.0.255`

Verification	On Router A, check the routing table and verify that only the entry 200.1.1.0/24 exists.
A	`A# show ip route rip` `R  200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`

Filtering the Sent RIP Routing Information

Scenario **Figure 1-16**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Enable the RIP routing process to advertise only the route 200.1.1.0/24.
B	B# configure terminal B(config)# router rip B(config-router)# redistribute connected B(config-router)# distribute-list 10 out B(config-router)# version 2 B(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Verification	Check the routing table on Router A, and verify that route in the 200.1.1.0 network segment exists.
A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

Common Errors

- Filtering fails because the filtering rules of the access list are not properly configured.

1.4.10 Modifying Route Selection Parameters

Configuration Effect

- Change the RIP 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 RIP routes.

Notes

- The RIP basic functions must be configured.

Configuration Steps

↘ **Modifying the Administrative Distance of a RIP Route**

- Optional.
- This configuration is mandatory if you wish to change the priorities of RIP routes on a router that runs multiple unicast routing protocols.

Increasing the Metric of a Received or Sent RIP Route

- Optional.
- Unless otherwise required, this configuration should be performed on a router where the metrics of routes need to be adjusted.

Configuring the Default Metric of an External Route Redistributed to RIP

- Optional.
- Unless otherwise required, this configuration must be performed on an ASBR to which external routes are introduced.

Verification

Run the **show ip rip** command to display the administrative distance currently configured. Run the **show ip rip data** command to display the metrics of redistributed routes to verify that the configuration takes effect.

Related Commands

Modifying the Administrative Distance of a RIP Route

Command Syntax	**distance** *distance* [*ip-address wildcard*]
Parameter Description	*distance*: Sets the administrative distance of a RIP route. The value is an integer ranging from 1 to 255. *ip-address*: Indicates the prefix of the source IP address of the route. *wildcard*: Defines the IP address comparison bit. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to configure the administrative distance of a RIP route.

Increasing the Metric of a Received or Sent RIP Route

Command Syntax	**offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the access list. **In**: Uses the ACL to modify the metric of a received route. **out**: Uses the ACL to modify the metric of a sent route. *offset*: Indicates the offset of the modified metric. The value ranges from 0 to 16. *interface-type*: Uses the ACL on the specified interface. *interface-number*: Specifies the interface number.

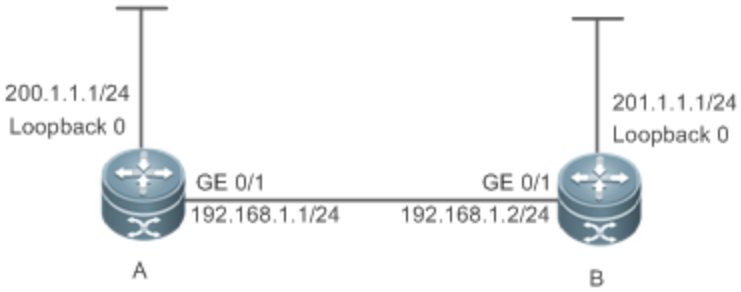
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to increase the metric of a received or sent RIP route. If the interface is specified, the configuration takes effect only on the specified interface; otherwise, the configuration takes effect globally.

Configuring the Default Metric of an External Route Redistributed to RIP

Command Syntax	**default-metric** *metric-value*
Parameter Description	*metric-value:* Indicates the default metric. The valid value ranges from 1 to 16. If the value is equal to or greater than 16, the system determines that this route is unreachable.
Command Mode	Routing process configuration mode
Configuration Usage	This command must be used together with the routing protocol configuration command **redistribute**.

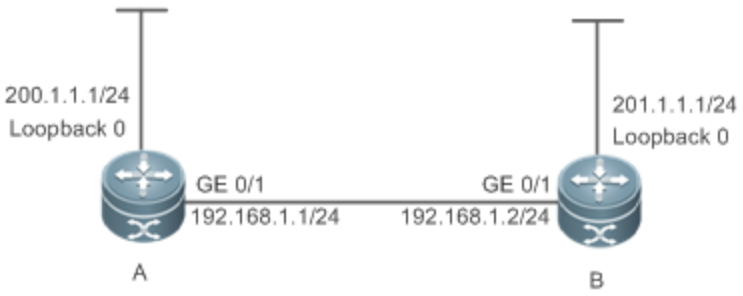
Configuration Example

Increasing the Metric of a Received or Sent RIP Route

Scenario Figure 1-17	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Increase by 7 the metric of each RIP route in the range specified by ACL 7. ● Increase by 7 the metric of each learned RIP route in the range specified by ACL 8.

A	`A# configure terminal`
	`A(config)# access-list 7 permit host 200.1.1.0`
	`A(config)# access-list 8 permit host 201.1.1.0`
	`A(config)# router rip`
	`A(config-router)# offset-list 7 out 7`
	`A(config-router)# offset-list 8 in 7`

Verification	Check the routing table on Router A and Router B to verify that the metrics of RIP routes are 8.

Scenario **Figure 1-17**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Increase by 7 the metric of each RIP route in the range specified by ACL 7. ● Increase by 7 the metric of each learned RIP route in the range specified by ACL 8.
A	A# configure terminal A(config)# access-list 7 permit host 200.1.1.0 A(config)# access-list 8 permit host 201.1.1.0 A(config)# router rip A(config-router)# offset-list 7 out 7 A(config-router)# offset-list 8 in 7
Verification	Check the routing table on Router A and Router B to verify that the metrics of RIP routes are 8.
A	A# show ip route rip R 201.1.1.0/24 [120/8] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	B# show ip route rip R 200.1.1.0/24 [120/8] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

1.4.11 Modifying Timers

Configuration Effect

- Change the duration of RIP timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- The RIP 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.

Configuration Steps

Modifying the Update Timer, Invalid Timer, and Flush Timer

This configuration must be performed if you need to adjust the RIP timers.

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol. For routers connected to the same network, values of the three RIP timers must be the same. Generally, you are advised not 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.

Unless otherwise required, this configuration should be performed on a router where RIP timers need to be modified.

Setting the Sending Delay Between RIP Route Update Packets

This configuration must be performed if you need to adjust the sending delay between RIP Update packets.

Run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all Update packets.

Unless otherwise required, this configuration should be performed on a router where the sending delay needs to be adjusted.

Verification

Run the **show ip rip** command to display the current settings of RIP timers.

Related Commands

Modifying the Update Timer, Invalid Timer, and Flush Timer

Command Syntax	**timers basic** *update invalid flush*
Parameter Description	*update*: Indicates the route update time in second. It defines the interval at which the device sends the route update packet. Each time an Update packet is received, the invalid timer and flush timer are reset. By default, a routing update packet is sent every 30s. *invalid*: Indicates the route invalid time in second, counted from the last time when a valid update packet is received. It defines the time after which the route in the routing list becomes invalid because the route is not updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no Update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the Update packet is received before the invalid timer expires, the timer is reset. The default duration of the invalid timer is 180s. *flush*: Indicates the route flushing time in second, counted from the time when the RIP route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Configuration	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

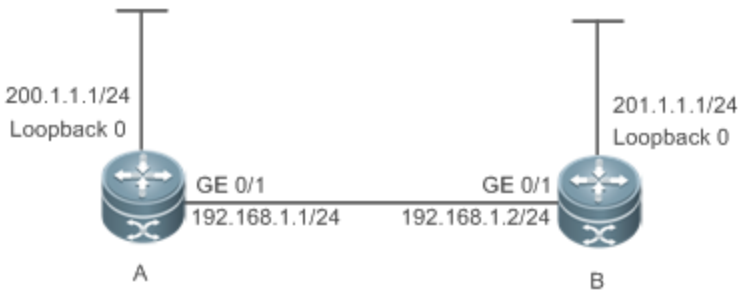
Usage	

Setting the Sending Delay Between RIP Route Update Packets

Command Syntax	**output-delay** *delay*
Parameter Description	*delay:* Sets the sending delay between packets in ms. The value ranges from 8 to 50.
Command Mode	Interface configuration mode
Configuration Usage	Normally, 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 not be able to process all update packets in time, causing a loss of routing information. In this case, you need to run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all update packets.

Configuration Example

Setting the Sending Delay Between RIP Route Update Packets

Scenario Figure 1-18	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure the sending delay of update packets on Router A.

A	`A# configure terminal`
	`A(config)# router rip`
	`A(config-router)# output-delay 30`

Verification	Capture packets on Router A and compare the sending time of update packets before and after the configuration, and verify that a delay of 30 ms is introduced.

Common Errors

For routers connected to the same network, values of the three RIP timers are not the same.

1.4.12 Enabling GR

Configuration Effect

- When a distributed route switches services from the active board to the standby board, traffic forwarding continues and is not interrupted.
- When the RIP process is being restarted, traffic forwarding continues and is not interrupted.

Notes

- The RIP basic functions must be configured.
- The GR period is at least twice the RIP route update period.
- During the RIP GR process, ensure that the network environment is stable.

Configuration Steps

↘ Configuring the GR Restarter Capability

This configuration must be performed if RIP needs to be gracefully restarted to ensure data forwarding during hot standby switchover.

The GR function is configured based on the RIP process. You can configure different parameters for different RIP processes based on the actual conditions.

The GR period is the maximum time from restart of the RIP process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIP route is restored so as to restore the RIP state before the restart. After the restart period expires, RIP exits from the GR state and performs common RIP operations.

Unless otherwise required, this configuration should be performed on every router that needs to be gracefully restarted.

Verification

- Run the **show ip rip** command to display the GR state and configured time.
- Trigger a hot standby switchover, and verify that data forwarding is not interrupted.

Related Commands

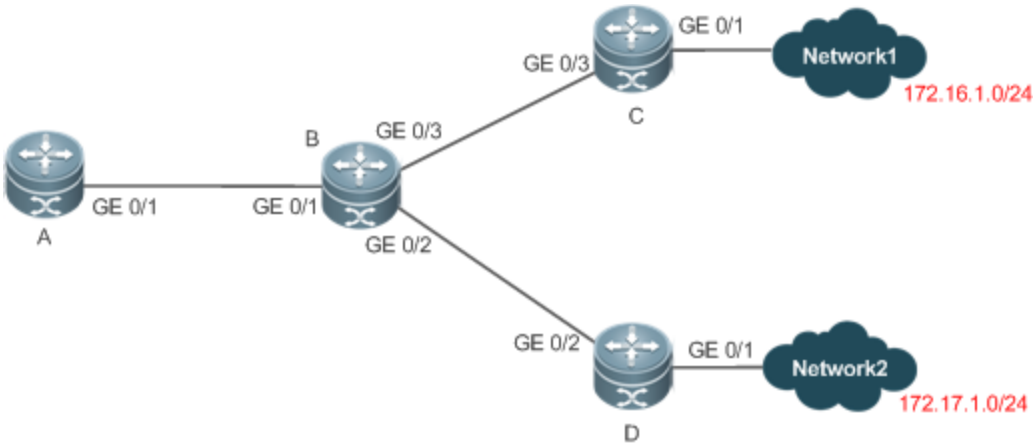
↘ Configuring the GR Restarter Capability

Command Syntax	**graceful-restart** [**grace-period** *grace-period*]
Parameter Description	**graceful-restart**: Enables the GR function. **grace-period**: Explicitly configures the grace period. *grace-period*: Indicates the GR period. The value ranges from 1s to 1800s. The default value is twice the update time or 60s, whichever is the smaller.
Command Mode	Routing process configuration mode

Configuration Usage	This command allows you to explicitly modify the GR period. Note that GR must be completed after the update timer of the RIP route expires and before the invalid timer of the RIP 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 advised not to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is longer than the duration of the update timer but shorter than the duration of the invalid timer based on the configuration of the **timers basic** command.

Configuration Example

Configuring the GR Restarter Capability

Scenario **Figure 1-19**	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1 C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2 D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router B, enable the GR function.

	`B# configure terminal`
	`B(config)# router rip`
	`B(config-router)# graceful-restart grace-period 90`

Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination Network 1 and Network 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination Network 1 from Router A, and verify that traffic forwarding is not interrupted during the switchover.

1.5 Monitoring

Displaying

Description	Command
Displays the basic information about a RIP process.	**show ip rip**
Displays the RIP routing table.	**show ip rip database** [*network-number network-mask*] [**count**]
Displays information about external routes redistributed by RIP.	**show ip rip external** [**connected**] | **ospf** *process-id* | **static**]
Displays the RIP interface information.	**show ip rip interface** [*interface-type interface-number*]
Displays the RIP neighbor information.	**show ip rip peer** [*ip-address*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs events that occur when the RIP process is running.	**debug ip rip event**
Debugs interaction with the NSM process.	**debug ip rip nsm**
Debugs the sent and received packets.	**debug ip rip packet** [**interface** *interface-type interface-number* | **recv** | **send**]
Debugs the RIP GR process.	**debug ip rip restart**
Debugs the route changes of the RIP process.	**debug ip rip route**

2 Configuring OSPFv2

2.1 Overview

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.

OSPF Version 2 (OSPFv2) is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.

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, notifications 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.

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be L3 switches, routers, or firewall.

Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv2.

Protocols and Standards

RFC2328	This memo documents version 2 of the OSPF protocol. OSPF is a link-state routing protocol.
RFC 2370	This memo defines enhancements to the OSPF protocol to support a new class of link-state advertisements (LSA) called Opaque LSAs. Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF.
RFC3137	This memo describes a backward-compatible technique that may be used by OSPF (Open Shortest Path First) implementations to advertise unavailability to forward transit traffic or to lower the preference level for the paths through such a router.

RFC3623	This memo documents an enhancement to the OSPF routing protocol, whereby an OSPF router can stay on the forwarding path even as its OSPF software is restarted.
RFC3630	This document describes extensions to the OSPF protocol version 2 to support intra-area Traffic Engineering (TE), using Opaque Link State Advertisements.
RFC3682	The use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to protect a protocol stack from CPU-utilization based attacks has been proposed in many settings.
RFC3906	This document describes how conventional hop-by-hop link-state routing protocols interact with new Traffic Engineering capabilities to create Interior Gateway Protocol (IGP) shortcuts.
RFC4576	This document specifies the necessary procedure, using one of the options bits in the LSA (Link State Advertisements) to indicate that an LSA has already been forwarded by a PE and should be ignored by any other PEs that see it.
RFC4577	This document extends that specification by allowing the routing protocol on the PE/CE interface to be the OSPF protocol.
RFC4750	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based Internets. In particular, it defines objects for managing version 2 of the Open Shortest Path First Routing Protocol. Version 2 of the OSPF protocol is specific to the IPv4 address family.

2.2 Applications

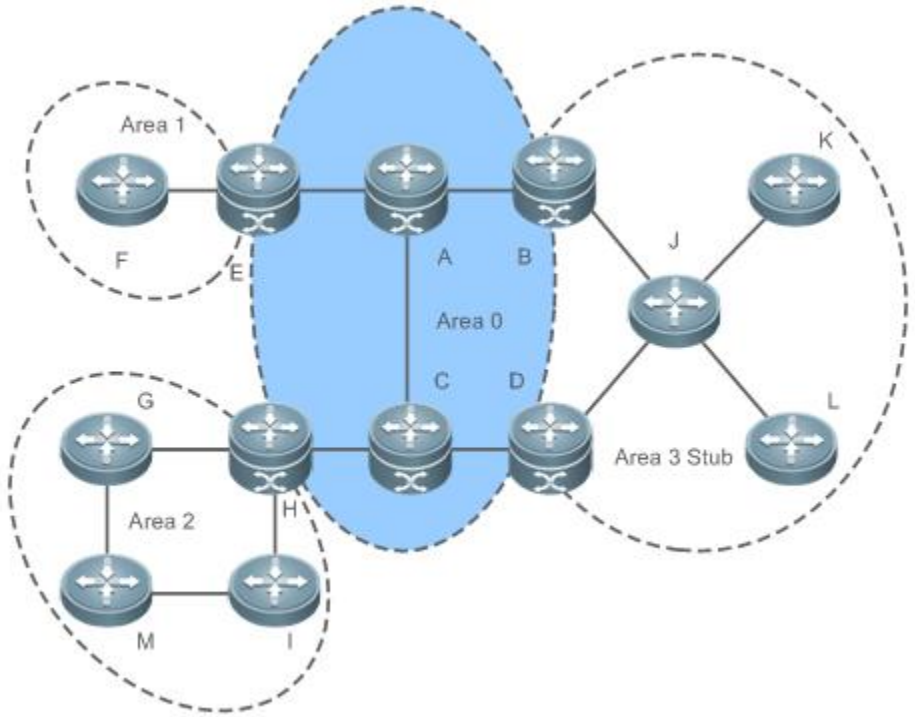
Application	Description
Intra-Domain Interworking	OSPF runs within the AS, which is divided into several areas.
Inter-Domain Interworking	Several ASs are interconnected. OSPF runs within each AS.

2.2.1 Intra-Domain Interworking

Scenario

OSPF runs within the AS. If the number of routers exceeds 40, it is recommended that the AS be divided into several areas. Generally, high-end devices featuring reliable performance and fast processing speed are deployed in a backbone area, and low-end or medium-range devices with relatively lower performance can be deployed in a normal area. All normal areas must be connected to the backbone area. It is recommended that a normal are allocated on the stub be configured as a stub area. As shown in Figure 2-1, the network is divided into four areas. Communication between these areas must go through the backbone area, that is, area 0.

Figure 2-1 Division of the OSPF Areas



Remarks	A, B, C, D, E, and H are located in the backbone area, and are backbone routers. Area 3 is configured as a stub area.

Deployment

- OSPF runs on all routers within the AS to implement unicast routing.

2.3 Features

Basic Concepts

Routing Domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, the AS is also called routing domain.

An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

OSPF Process

OSPF supports multiple instances, and each instance corresponds to an OSPF process.

One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.

The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.

Router ID

The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.

If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

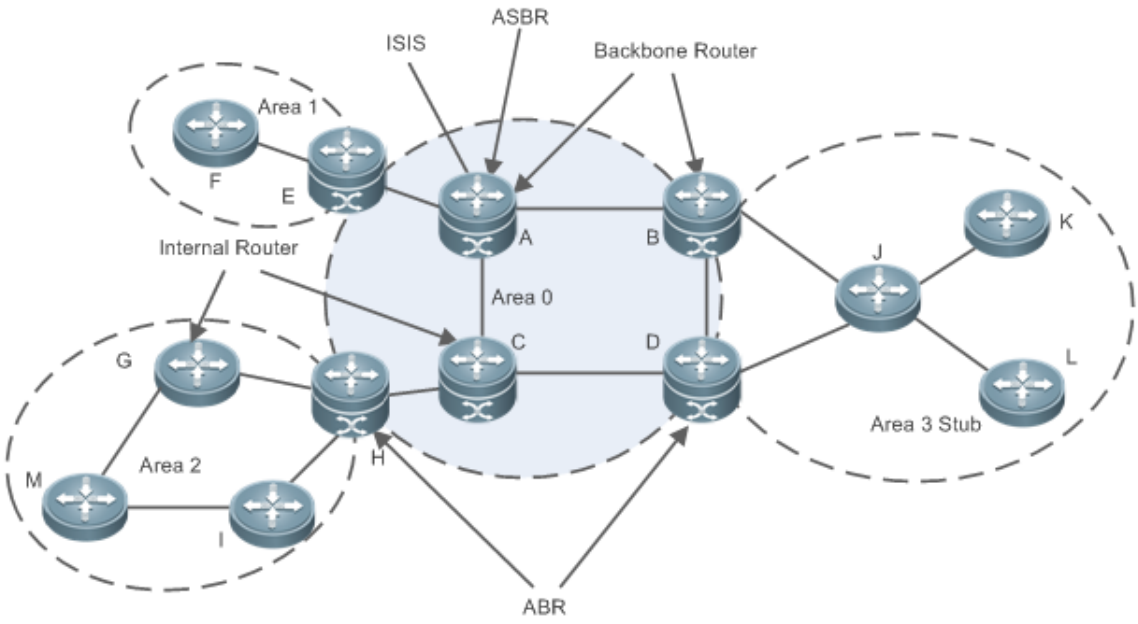
Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.

Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

Figure 2-2 Division of the OSPF Areas



OSPF Router

The following types of routers are defined in OSPF, and assigned with different responsibilities:

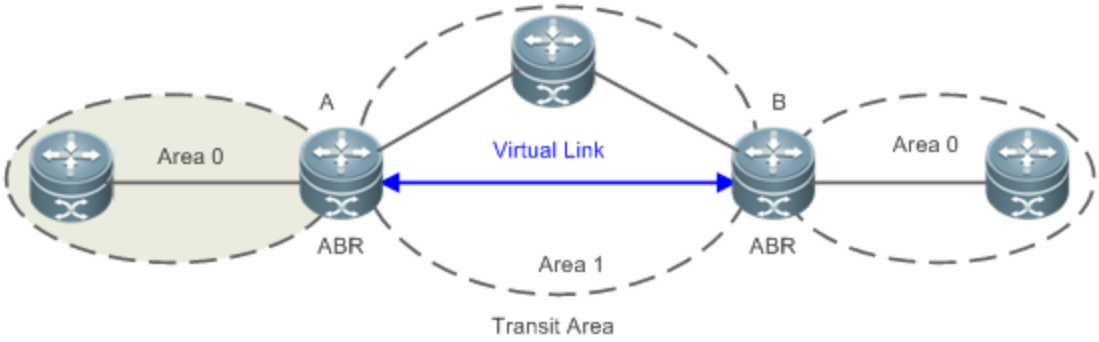
- Internal router
- All interfaces of an interval router belong to the same OSPF area. As shown in Figure 2-2, A, C, F, G, I, M, J, K, and L are internal routers.
- Area border router (ABR)

- 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. As shown in Figure 2-2, B, D, E, and H are ABRs.
- 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. As shown in Figure 2-2, A, B, C, D, E, and H are backbone routers.
- AS boundary router (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. As shown in Figure 2-2, A is an ASBR.

Virtual Link

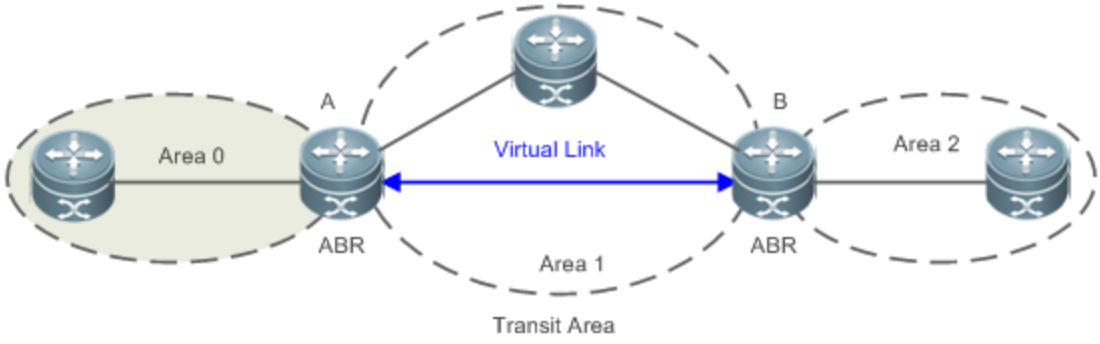
OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

Figure 2-3 Discontinuous Backbone Area on the Physical Network



As shown in Figure 2-3, a virtual link is set up between A and B to connect two separated area 0s. Area 1 is a transit area, and A and B are ABRs of Area 1.

Figure 2-3 Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 2-3, 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 0 and area 2.

LSA

OSPF describes the routing information by means of Link State Advertisement (LSA).

LSA Type	Description
Router-LSA(Type 1)	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(Type 2)	This LSA is originated by a designated routers (DR) on the 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 or Not-So-Stubby Area (NSSA) areas.
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 areas where the ASBR is located.
AS-external-LSA(Type 5)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised to all areas except the stub and NSSA areas.
NSSA LSA(Type 7)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised only within the NASSA areas.
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 only advertised within the network segment where interfaces resides. The Grace LSA used to support graceful restart (GR) is one of Type 9 LSAs. ● Type 10 LSAs are advertised within an area. The LSA used to support Traffic Engineering (TE) is one of Type 10 LSAs. ● Type 11 LSAs are advertised within an AS. At present, there are no application examples of Type 11 LSAs.

Stub areas, NSSA areas, totally stub areas, and totally NSSA areas are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPF routes.

OSPF Packet

The following table lists the protocol packets used by OSPF. These OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
Database Description (DD)	DD packets carry brief information about the local Link-State Database (LSDB) and are used to synchronize the LSDBs between OSPF neighbors.
Link State Request (LSR)	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.

Link State Update (LSU)	LSU packets are used to send the required LSAs to peers.
Link State Acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs.

Overview

Feature	Description
Link-State Routing Protocols	Run OSPF on the router to obtain routes to different destinations on the network.
OSPF Route Management	Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.
Enhanced Security and Reliability	Use functions such as authentication to enhance security, stability, and reliability of OSPF.
Network Management	Use functions such as the management information base (MIB) and Syslog to facilitate OSPF management.

2.3.1 Link-State Routing Protocols

OSPF is a type of link-state routing protocols. Its working process is as follows:

- Neighbor discovery → Bidirectional communication
- An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.
- Database synchronization → Full adjacency
- A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.
- 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.

Working Principle

↘ Neighbor Discovery → Bidirectional Communication

Routers send Hello packets through all OSPF-enabled interfaces (or virtual links). If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutually neighbors find their own router IDs from Hello packets sent from neighbors, and bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- Router ID of the originating router
- Area ID of the originating router interface (or virtual link)
- Subnet mask of the originating router interface (or virtual link)
- Authentication information of the originating router interface (or virtual link)
- Hello interval of the originating router interface (or virtual link)

- Neighbor dead interval of the originating router interface (or virtual link)
- Priority of the originating router interface (used for DR/BDR election)
- IP addresses of the DR and Backup Designated Router (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.

OSPF will be very quiet without changes in link costs 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 costs. OSPF generates a routing table based on the SPT.

If changes in link costs or network addition or deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

The Dijkstra algorithm is used to find a shortest path from a vertex to other vertices in a weighted directed graph.

OSPF Network Types

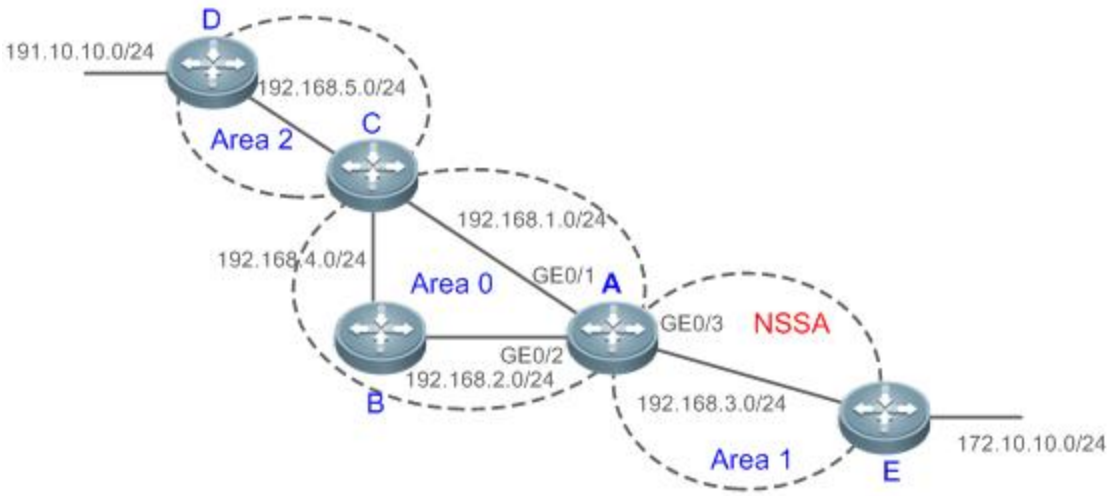
A router does not necessarily need to exchange LSAs with every neighbor and set up an adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency:

- Broadcast
- 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.
- Ethernet and fiber distributed data interface (FDDI) belong to the broadcast network type by default.
- Non-broadcast multiple access (NBMA)
- 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.

- X.25, frame relay, and ATM belong to NBMA networks by default.
- Point-to-point (P2P)
- 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.
- PPP, HDLC, and LAPB belongs to the P2P network type by default.
- Point-to-multipoint (P2MP)
- 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.
- Networks without any link layer protocol belong to the P2MP network type by default. P2MP broadcast
- 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.
- Networks without any link layer protocol belong to the P2MP network type by default.

OSPF Route Types

Figure 2-4



Display the OSPF routes (marked in red) in the routing table of Router A.

```
A#show ip route


Codes:  C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00,GigabitEthernet 0/3
O E2 191.10.10.0/24 [110/20] via 192.168.1.2, 01:11:26,GigabitEthernet 0/1
C    192.168.1.0/24 is directly connected,GigabitEthernet 0/1
C    192.168.1.1/32 is local host.
C    192.168.2.0/24 is directly connected,GigabitEthernet 0/2
C    192.168.2.1/32 is local host.
C    192.168.3.0/24 is directly connected,GigabitEthernet 0/3
C    192.168.3.1/32 is local host.
O    192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02,GigabitEthernet 0/2
O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:02,GigabitEthernet 0/1
```

This series does not support ISIS or BGP. The configuration example is only for reference.

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: Intra-area route
- This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- IA: Inter-area route
- This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- E1: Type 1 external route
- This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- E2: Type 2 external route
- This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- N1: Type 1 external route of the NSSA area
- This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

- N2: Type 2 external route of the NSSA area
- This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

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.

Related Configuration

Enabling OSPF

OSPF is disabled by default.

Run the **router ospf** 1 command to create an OSPF process on the router.

Run the **network area** command to enable OSPF on the interface and specify the area ID.

Run the **area virtual-link** command to create a virtual link on the router. The virtual link can be treated as a logical interface.

Router ID

By default, the OSPF process elects the largest IP address among the IP addresses of 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 IP address among the IP addresses of all the loopback interfaces as the router ID.

Alternatively, you can run the **router-id** command to manually specify the router ID.

Protocol Control Parameters

Run the **ip ospf hello-interval** command to modify the Hello interval on the interface. The default value is 10s (or 30s for NBMA networks).

Run the **ip ospf dead-interval** command to modify the neighbor dead interval on the interface. The default value is four times the Hello interval.

Use the **poll-interval** parameter in the **neighbor** command to modify the neighbor polling interval on the NBMA interface. The default value is 120s.

Run the **ip ospf transmit-delay** command to modify the LSU packet transmission delay on the interface. The default value is 1s.

Run the **ip ospf retransmit-interval** command to modify the LSU packet retransmission interval on the interface. The default value is 5s.

Use the **hello-interval** parameter in the **area virtual-link** command to modify the Hello interval on the virtual link. The default value is 10s.

Use the **dead-interval** parameter in the **area virtual-link** command to modify the neighbor dead interval on the virtual link. The default value is four times the Hello interval.

Use the **transmit-delay** parameter in the **area virtual-link** command to modify the LSU packet transmission delay on the virtual link. The default value is 1s.

Use the **retransmit-interval** parameter in the **area virtual-link** command to modify the LSU packet retransmission interval on the virtual link. The default value is 5s.

Run the **timers throttle lsa all** command to modify parameters of the exponential backoff algorithm that generates LSAs. The default values of these parameters are 0 ms, 5000 ms, and 5000 ms.

Run the **timerspacinglsa-group** command to modify the LSA group update interval. The default value is 30s.

Run the **timers pacing lsa-transmit** command to modify the LS-UPD packet sending interval and the number of sent LS-UPD packets. The default values are 40 ms and 1.

Run the **timers lsa arrival** command to modify the delay after which the same LSA is received. The default value is 1000 ms.

Run the **timers throttle spf** command to modify the SPT computation delay, minimum interval between two SPT computations, and maximum interval between two SPT computations. The default values are 1000 ms, 5000 ms, and 10000 ms.

↘ 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.

Run the **ip ospf network** command to manually specify the network type of an interface.

Run the **neighbor** command to manually specify a neighbor. For the NBMA and P2MP non-broadcast types, you must manually specify neighbors.

Run the **ip ospf priority** command to adjust the priorities of interfaces, which are used for DR/BDR election. The DR/BDR election is required for the broadcast and NBMA types. The router with the highest priority wins in the election, and the router with the priority of 0 does not participate in the election. The default value is 1.

2.3.2 OSPF Route Management

Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Working Principle

↘ (Totally) Stub Area and (Totally)NSSA Area

The (totally) stub and (totally) NSSA areas help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a (totally) stub or NSSA area, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Area	Type1 and Type2 LSAs	Type 3 LSA	Type 4 LSA	Type 5 LSA	Type 7 LSA
Non (totally) stub area and NSSA area	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one	Not allowed	Not allowed	Not allowed

		default route)			
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA area	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA area	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

- The ABR uses Type 3LSAs to advertise a default route to the (totally) stub or NSSA area.
- The ABR converts Type 7 LSAs in the totally NSSA area to Type 5LSAs, and advertise Type5LSAs to the backbone area.

- If an area is appropriately configured as a (totally) stub area or an NSSA area, a large number of E1, E2, and IA routes will not be added to the routing table of a router in the area.

Area	Routes Available in the Routing Table of a Router Inside the Area
Non (totally) stub area and NSSA area	O: a route to a destination network in the local area IA: a route to a destination network in another area E1 or E2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area IA: a default route
NSSA area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)
Totally NSSA area	O: a route to a destination network in the local area IA: a default route N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)

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.

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 Type3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs. If continuous network segments exist, it is recommended that you configure route summarization.

When configuring route summarization, the summarization range may exceed the actual network scope of routes. 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, the ABR or ASBR automatically adds a discard route to the routing table. This route will not be advertised.

Route Filtering

OSPF supports route filtering to ensure security and facilitate control when the routing information is being learned, exchanged, or used.

Using configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSAs) or exchanging routing information (any LSAs) with neighbors.
- Routing information advertised between areas: Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).
- 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.

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.

Using configuration commands, you can modify the 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

Both the cost and the metric indicate the cost and are not differentiated from each other.

OSPF Administrative Distance

The administrative distance (AD) evaluates reliability of a route, and the 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.

Route Source	Directly-Connected Network	Static Route	OSPF Route	RIP Route	Unreachable Route
Default AD	0	1	110	120	255

Related Configuration

Stub Area and NSSA Area

No stub or NSSA area is configured by default.

Run the **area stub** command to configure a specified area as a stub area.

Run the **area nssa** command to configure a specified area as an NSSA area.

The backbone area cannot be configured as a stub or an NSSA area.

A transit area (with virtual links going through) cannot be configured as a stub or an NSSA area.

An area containing an ASBR cannot be configured as a stub area.

Route Redistribution and Default Route Introduction

By default, routes are not redistributed and the default route is not introduced.

Run the **redistribute** command to configure route redistribution.

Run the **default-information originate** command to introduce the default route.

After configuring route redistribution and default route introduction, the route automatically becomes an ASBR.

Route Summarization

By default, routes are not summarized. If route summarization is configured, a discard route will be automatically added.

Run the **arearange** command to summarize routes distributed between areas (Type 3 LSA) on the ABR.

Run the **summary-address** command to summarize redistributed routes (Type 5 and Type 7 LSAs) on the ASBR.

Run the **discard-route** command to add a discard route to the routing table.

Route Filtering

By default, routes are not filtered.

Run the **passive-interface** command to configure a passive interface. Routing information (any LSAs) cannot be exchanged on a passive interface.

Run the **ip ospfdatabase-filter all out** command to prohibit an interface from sending routing information (any LSAs).

Run the **area filter-list** command to filter routing information advertised between areas on the ABR. Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).

Use the **route-map** parameter in the **redistribute** command, or use the **distribute-list out** command to filter the external routing information of the AS on the ASBR. Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).

Run the **distribute-list in** command to filter LSAs received by the router. In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

- Cost from the interface to the directly-connected network segment (cost on the interface)
- The default value is the auto cost. Auto cost = Reference bandwidth/Interface bandwidth
- Run the **auto-cost reference-bandwidth** command to set the reference bandwidth of auto cost. The default value is 100 Mbps.
- Run the **ip ospf cost** command to manually set the cost of the interface. The configuration priority of this item is higher than that of the auto cost.
- Cost from the interface to a specified neighbor (that is, cost from the local device to a specified neighbor)
- The default value is the auto cost.
- Use the **cost** parameter in the **neighbor** command to modify the cost from the interface to a specified neighbor. The configuration priority of this item is higher than that of the cost of the interface.
- This configuration item is applicable only to P2MP-type interfaces.
- Cost from the ABR to the inter-area summarization network segment (that is, the cost of the summarized inter-area route)
- If OSPF routing is compatible with RFC1583, the default value is the minimum cost among all costs of the summarized links; otherwise, the default value is the maximum cost among all costs of the summarized links.
- Run the **compatible rfc1583** command to make OSPF routing compatible with RFC1583. By default, OSPF routing is compatible with RFC1583.
- Use the **cost** parameter in the **area range** command to modify the cost of inter-area route summarization.
- Cost from the ABR to the default network segment (that is, the cost of the default route that is automatically advertised by the ABR to the stub or NSSA areas)

- The default value is 1.
- Run the **area default-cost** command to modify the cost of the default route that the ABR automatically advertise to the stub or NSSA areas.
- Cost from the ASBR to an external network segment (that is, the metric of an external route)
- By default, the metric of other types of redistributed routes is 20, and the route type is Type 2 External.
- Run the **default-metric** command to modify the default metric of the external route.
- Use the **metric**, **metric-type** and **route-map** parameters in the **redistribute** command to modify the metric and route type of the external route.
- Cost from the ASBR to the default network segment (that is, the metric of the default route that is manually introduced)
- By default, the metric is 1, and the route type is Type 2 External.
- Use the **metric**, **metric-type** and **route-map** parameters in the **default-information originate** command to modify the metric and route type of the default route that is manually introduced.
- Use the **metric** and **metric-type** parameters of **default-information originate** in the **area nssa** command to modify the metric and type of the default route that is manually introduced to the NSSA area.
- Run the **max-metric router-lsa** command to set metrics of all routes advertised on the router to the maximum value. In this way, the total cost of any path that passes through this router will become very large, and the path can hardly become the shortest path.

↘ OSPF Administrative Distance

By default, the OSPF AD is 110.

Run the **distance** command to set the AD of an OSPF route.

2.3.3 Enhanced Security and Reliability

Use functions such as authentication to enhance security, stability, and reliability of OSPF.

Working Principle

↘ 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 the adjacency cannot 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.

↘ MTU Verification

On receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as the MTU of the local interface. If the MTU of the interface specified in the received DD packet is greater than the MTU of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

Source Address Verification

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In particular, OSPF 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, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Two-Way Maintenance

OSPF routers periodically send Hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying too much 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 OSPF process, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

Overflow

OSPF requires that routers in the same area store the same LSDB. The number of routers keeps increasing on the network. Some routers, however, cannot store so much routing information due to the limited system resources. The large amount of routing information may exhaust the system resources of routers, causing failures of the routers.

The overflow function limit the number of external routes in the LSDB to control the size of the LSDB.

When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

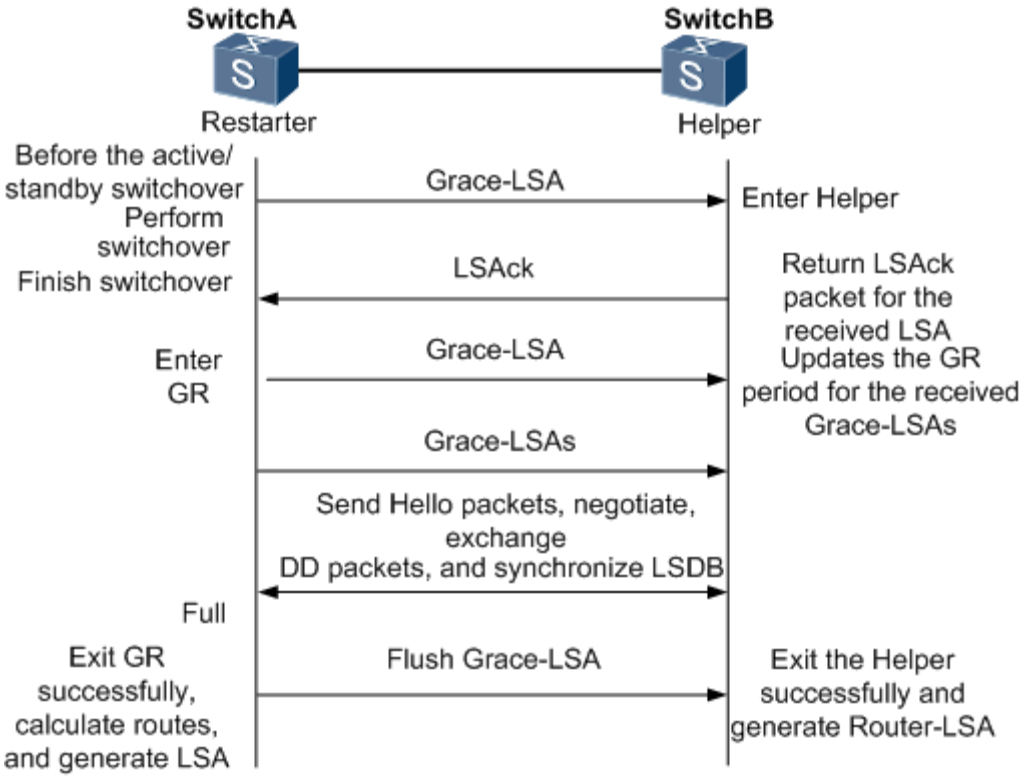
GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In

addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 2-5 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.

Fast Hello, BFD Correlation, and Fast Reroute

After a link fault occurs, OSPF senses the death of the neighbor only after a period of time (about 40s). 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 death of a neighbor within 1s once a link is faulty. This greatly accelerates route convergence and prevents traffic interruption.

Related Configuration

OSPF Packet Authentication

By default, authentication is disabled.

- Run the **area authentication** command to enable the authentication function in the entire area so that the function takes effect on all interfaces in this area. If authentication is enabled in area 0, the function takes effect on the virtual link.
- Run the **ip ospf authentication** command to enable authentication on an interface. This configuration takes precedence over the area-based configuration.
- Run the **ip ospf authentication-key** command to set the text authentication key on an interface.
- Run the **ip ospf message-digest-key** command to set the message digest 5 (MD5) authentication key on an interface.
- Use the **authentication** parameter in the **area virtual-link** command to enable authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.
- Use the **authentication-key** parameter in the **area virtual-link** command to set the text authentication key at both ends of a virtual link.
- Use the **message-digest-key** parameter in the **area virtual-link** command to set the MD5 authentication key at both ends of a virtual link.

MTU Verification

By default, MTU verification is disabled.

Run the **ip ospf mtu-ignore** command to disable MTU verification on an interface.

Source address verification

By default, source address verification is enabled on a P2P interface.

Run the **ip ospf source-check-ignore** command to disable source address verification on an interface.

Two-Way Maintenance

By default, bidirectional maintenance is enabled.

Run the **two-way-maintain** command to enable two-way maintenance.

Concurrent neighbor Interaction Restriction

Run the **max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with the current OSPF process. The default value is 5.

Run the **ip router ospf max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with all OSPF processes on the router. The default value is 10.

Overflow

Run the **overflow memory-lack** command to allow the router to enter the overflow state when the memory is insufficient. By default, the router is allowed to enter the overflow state when the memory is insufficient.

Run the **overflow database** command to allow the router to enter the overflow state when the number of LSAs is too large. By default, the router is not allowed to enter the overflow state when the number of LSAs is too large.

Run the **overflow database external** command to allow the router to enter the overflow state when the number of external LSAs is too large. By default, the router is not allowed to enter the overflow state when the number of external-LSAs is too large.

GR

By default, the restarter function is disable, and the helper function is enabled.

Run the **graceful-restart** command to configure the restarter function.

Run the **graceful-restart helper** command to configure the helper function.

Fast Hello

By default, the neighbor dead interval on the interface is 40s.

Run the **ip ospf dead-interval minimal hello-multiplier** command to enable the Fast Hello function on an interface, that is, the neighbor dead interval is 1s.

2.3.4 Network Management

Use functions such as the MIB and Syslog to facilitate OSPF management.

Working Principle

MIB

MIB is the device status 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 with 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 proactively 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.

Related Configuration

MIB

By default, the MIB is bound with the OSPF process with the smallest process ID.

Run the **enable mib-binding** command to bind the MIB with the current OSPF process.

Trap

By default, all traps are disabled, and the device is not allowed to send OSPF traps.

Run the **enable traps** command to enable a specified trap for an OSPF process.

Run the **snmp-server enable traps ospf** command to allow the device to send OSPF traps.

SYSLOG

By default, the Syslog is allowed to record the adjacency changes.

Run the **log-adj-changes** command to allow the Syslog to record the adjacency changes.

2.4 Configuration

Configuration	Description and Command	
Configuring OSPF Basic Functions	(Mandatory) It is used to build an OSPF routing domain.	
	router ospf	Creates an OSPF process.
	router-id	Configures a router ID.
	network area	Enables OSPF on an interface and specifies an area ID.
	area virtual-link	Creates a virtual link.
Setting the Network Type	(Optional) The configurations are mandatory if the physical network is the X.25, frame relay, or ATM network.	
	ip ospf network	Defines the network type.
	neighbor	Specifies a neighbor.
	ip ospf priority	Configures the DR priority.
Configuring Route Redistribution and Default Route	(Optional) The configurations are recommended if the OSPF routing domain is connected with an external network.	
	redistribute	Configures route redistribution.
	default-information originate	Introduces a default route.
Configuring Stub Area and NSSA Area	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	areastub	Configures a stub area.
	areanssa	Configures an NSSA area.

Configuration	Description and Command	
Configuring Route Summarization	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	area range	Summarizes routes that are advertised between areas.
	summary-address	Summarizes routes that are introduced through redistribution.
	discard-route	Adds a discard route to the routing table.
Configuring Route Filtering	(Optional) It is used to manually control interaction of routing information and filter available OSPF routes.	
	passive-interface	Configures a passive interface.
	ip ospf database-filter all out	Prohibits an interface from sending LSAs.
	area filter-list	Filters routes that are advertised between areas.
	distribute-list out	Filters routes that are introduced through redistribution.
	distribute-list in	Filters routes that are calculated based on the received LSAs.
Modifying Route Cost and AD	(Optional) It is used to manually control the shortest route computed by OSPF and determine whether to select an OSPF route preferentially.	
	auto-cost reference-bandwidth	Modifies the reference bandwidth of the auto cost.
	ip ospf cost	Modifies the cost in the outbound direction of an interface.
	area default-cost	Modifies the cost of the default route in a stub or an NSSA area.
	default-metric	Modifies the default metric of a redistributed route.
	max-metric router-lsa	Configures the maximum metric.
	compatible rfc1583	Enables the routing rules to be compatible with RFC1583.
	distance	Modifies the OSPF AD.
Enabling Authentication	(Optional) It is used to prevent routers that illegally access the network and hosts that forge OSPF packets from participating in the OSPF protocol process.	
	area authentication	Enables authentication and sets the authentication mode in an area.
	ip ospf authentication	Enables authentication and sets the authentication mode on an interface.

Configuration	Description and Command	
	ip ospf authentication-key	Sets the text authentication key on an interface.
	ip ospfmessage-digest-keymd5	Sets the MD5 authentication key on an interface.
Enabling Overflow	⚠ (Optional) It is used to prevent the problem that OSPF processes stop running due to over-consumption of the memory.	
	overflow memory-lack	Allows the router to enter the overflow state when the memory is insufficient.
	overflow database	Allows the router to enter the overflow state when the number of LSAs exceeds the preset limit.
	overflow database external	Allows the router to enter the overflow state when the number of external LSAs exceeds the preset limit.
Modifying the Maximum Number of Concurrent Neighbors	⚠ (Optional) It is used to prevent the problem of performance deterioration caused by over-consumption of the CPU.	
	max-concurrent-dd	Modifies the maximum number of con current neighbors on the current OSPF process.
	router ospf max-concurrent-dd	Modifies the maximum number of con current neighbors on all OSPF processes.
Disabling Source Address Verification	⚠ (Optional) It is used to prevent the problem that the adjacency cannot be set up due to the failure to obtain the peer address.	
	ip ospf source-check-ignore	Disables source address verification on an interface.
Disabling MTU Verification	⚠ (Optional) It is used to prevent the problem that the adjacency cannot be set up due to MTU inconsistency on the neighbor interface.	
	ip ospf mtu-ignore	Disables MTU verification on an interface.
Enabling Two-Way Maintenance	⚠ (Optional) It is used to prevent termination of the adjacency due to the delay or loss of Hello packets.	
	two-way-maintain	Enables two-way maintenance.
Enabling GR	⚠ (Optional) It is used to retain OSPF routing forwarding during restart or active/standby switchover of the OSPF processes to prevent traffic interruption.	
	graceful-restart	Configures the restarter function.
	graceful-restart helper	Configures the helper function.

Configuration	Description and Command	
Enabling Fast Hello	⚠ (Optional) It is used to quickly discover the death of a neighbor to prevent traffic interruption when a link is faulty.	
	ip ospf dead-interval minimal hello-multiplier	Enabling the Fast Hello function on an interface.
Configuring the Network Management Function	⚠ (Optional) The configurations enable users to use the SNMP network management software to manage OSPF.	
	enable mib-binding	Binds the MIB with the current OSPF process.
	enable traps	Enables a specified trap for an OSPF process.
	snmp-server enable traps ospf	Allows the device to send OSPF traps.
	log-adj-changes	Allows the Syslog to record the adjacency changes.
Modifying Protocol Control Parameters	⚠ (Optional) You are advised not to modify protocol control parameters unless necessary.	
	ip ospf hello-interval	Modifies the Hello interval.
	ip ospf dead-interval	Modifies the neighbor death interval.
	timers throttle lsa all	Modifies parameters of the exponential backoff algorithm that generates LSAs.
	timers throttle route inter-area	Modifies the inter-area route computation delay.
	timers throttle route ase	Modifies the external route computation delay.
	timerspacinglsa-group	Modifies the LSA group update interval.
	timers pacing lsa-transmit	Modifies the LS-UPD packet sending interval.
	ip ospf transmit-delay	Modifies the LSU packet transmission delay.
	ip ospf retransmit-interval	Modifies the LSU packet retransmission interval.
	timers lsa arrival	Modifies the delay after which the same LSA is received.
	timers throttlespf	Modifies the SPT computation timer.

2.4.1 Configuring OSPF Basic Functions

Configuration Effect

- Set up an OSPF routing domain on the network to provide IPv4 unicast routing service for users on the network.

Notes

- Ensure that the IP unicast routing function is enabled, that is, **ip routing** is not disabled; otherwise, OSPF cannot be enabled.
- It is strongly recommended that you 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 network.

Configuration Steps

Creating an OSPF Process

- Mandatory.
- The configuration is mandatory for every router.

Configuring a Router ID

- (Optional) It is strongly recommended that you manually configure the router ID.
- If the router ID is not configured, OSPF selects an interface IP address. If the IP address is not configured for any interface, or the configured IP addresses have been used by other OSPF instances, you must manually configure the router ID.

Enabling OSPF on an Interface and Specifying an Area ID

- Mandatory.
- The configuration is mandatory for every router.

Verification

- Run the **show ip route ospf** command to verify that the entries of the OSPF routing table are correctly loaded.
- Run the **ping** command to verify that the IPv4 unicast service is correctly configured.

Related Commands

Creating an OSPF Process

Command	**router ospf** *process-id*
Parameter Description	*process-id:* Indicates the OSPF process ID. If the process ID is not specified, the process ID is 1.
Command Mode	Global configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently.

Configuring a Router ID

Command	**router-id** *router-id*
Parameter	*router-id:* Indicates the router ID to be configured. It is expressed in the IP address.

Description	
Command Mode	OSPF routing process configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently. Each OSPF process uses a unique router ID.

Enabling OSPF on an Interface and Specifying an Area ID

Command	**network** *ip-address wildcard* **area** *area-id*
Parameter Description	*ip-address*: Indicates the IP address of the interface. *wildcard:* Indicates the IP address comparison mode. **0** indicates accurate matching, and **1** indicates that no comparison is performed. *area-id:* Indicates the ID of an OSPF area. An OSPF area is always associated with an address range. To facilitate management, you can use a subnet as the ID of an OSPF area.
Command Mode	OSPF routing process configuration mode
Usage Guide	By defining *ip-address* and *wildcard*, you can use one command to associate multiple interfaces with one OSPF area. To run OSPF on one interface, you must include the primary IP address of the interface in the IP address range defined by **network area**. If the IP address range defined by **network area** contains only the secondary IP address of the interface, OSPF does not run on this interface. If the interface address matches the IP address ranges defined in the **network** commands of multiple OSPF processes, the OSPF process that the interface is associated with is determined based on the best match method.

Creating a Virtual Link

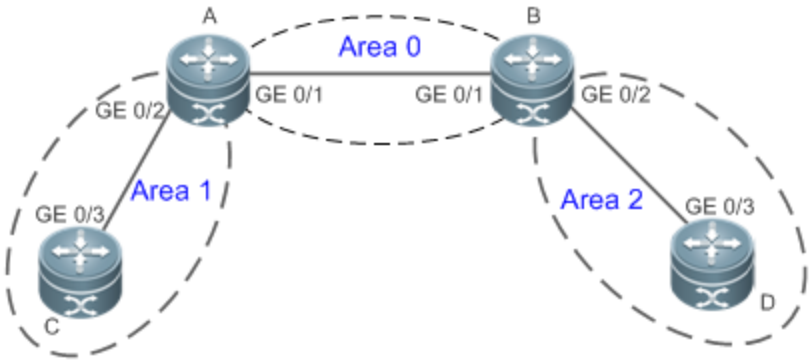
Command	**area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest**	**null**]] [**dead-interval**{ *seconds* |**minimal hello-multiplier** *multiplier*}] [**hello-interval***seconds*] [**retransmit-interval***seconds*] [**transmit-delay***seconds*] [[**authentication-key**[**0** |**7**]*key*]	[**message-digest-key***key-id* **md5**[**0** |**7**]*key*]]
Parameter Description	*area-id:* Indicates the ID of the OSPF transit area. The area ID can be a decimal integer or an IP address. *router-id:* Indicates the ID of a neighbor router on the virtual link. **dead-interval***seconds:* Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647. The setting of this parameter must be consistent with that on a neighbor. **minimal:** Indicates that the Fast Hello function is enabled to set the dead interval to 1s. **hello-multiplier:** Indicates the result of the dead interval multiple by the Hello interval in the Fast Hello function. *multiplier:* Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20. **hello-interval** *seconds:* Indicates the interval at which OSPF sends the Hello packet to the virtual link. The unit is second. The value ranges from 1 to 65,535. The setting of this parameter must be consistent with that on a neighbor. **retransmit-interval** *seconds:* Indicates the OSPF LSA retransmission time. The unit is second. The value ranges from 1 to 65,535.

	transmit-delay *seconds:* Indicates the delay after which OSPF sends the LSA. The unit is second. The value ranges from 1 to 65,535. **authentication-key** [**0** | **7**]*key:* Defines the key for OSPF plain text authentication. **message-digest-key** *key-id* **md5** [**0** | **7**]key: Defines the key ID and key for OSPF MD5 authentication. **authentication:** Sets the authentication type to plain text authentication. **message-digest:** Sets the authentication type to MD5 authentication. **null:** Indicates that authentication is disabled.
Command Mode	OSPF routing process configuration mode
Usage Guide	In the OSPF routing domain, all 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 area cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas. **router-id** is the ID of an OSPF neighbor router. If you are sure about the value of **router-id**, run the **show ip ospf neighbor** command to confirm the value. You can configure the loopback address as the router ID. The **area virtual-link** command defines only the authentication key of the virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, you must run the **area authentication** command. OSPF supports the Fast Hello function. After the OSPF Fast Hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF Fast Hello function by specifying the **minimal** and **hello-multiplier** keywords and the **multiplier** parameter. The **minimal** keyword indicates that the death interval is set to 1s, and **hello-multiplier** indicates the number of Hello packets sent per second. In this way, the interval at which the Hello packet is sent decreases to less than 1s. 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 death interval must be consistent and the **hello-multiplier** values can be inconsistent on routers at both ends of the virtual link. Ensure that at least one Hello packet can be received within the death interval. Run the **show ip ospf virtual-links** command to monitor the death interval and Fast Hello interval configured for the virtual link. The **dead-interval minimal hello-multiplier** and **hello-interval** parameters introduced for the Fast Hello function cannot be configured simultaneously.

Configuration Example

Scenario

Figure 2-6



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/3 192.168.2.2 D: GE 0/3 192.168.3.2

Configuration Steps

- Configure the interface IP addresses on all routers.
- Enable the IPv4 unicast routing function on all routers. (This function is enabled by default.)
- Configure the OSPF instances and router IDs on all routers.
- Enable OSPF on the interfaces configured on all routers.

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)#exit
A(config)#interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0
A(config-if-GigabitEthernet 0/2)#exit
A(config)#router ospf 1
A(config-router)#router-id192.168.1.1
A(config-router)#network 192.168.1.0 0.0.0.255 area 0
A(config-router)#network 192.168.2.0 0.0.0.255 area 1
```

B

```
B#configure terminal
B(config)#interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0
B(config-if-GigabitEthernet 0/1)#exit
B(config)#interface GigabitEthernet 0/2
```

	B(config-if-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)#exit B(config)#router ospf 1 B(config-router)#router-id192.168.1.2 B(config-router)#network 192.168.1.0 0.0.0.255 area 0 B(config-router)#network 192.168.3.0 0.0.0.255 area 2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ip address 192.168.2.2 255.255.255.0 C(config-if-GigabitEthernet 0/3)#exit C(config)#router ospf 1 C(config-router)#router-id192.168.2.2 C(config-router)#network 192.168.2.0 0.0.0.255 area 1
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ip address 192.168.3.2 255.255.255.0 D(config-if-GigabitEthernet 0/3)#exit D(config)#router ospf 1 D(config-router)#router-id192.168.3.2 D(config-router)#network 192.168.3.0 0.0.0.255 area 2
Verification	● Verify that the OSPF neighbors are correct on all routers. ● Verify that the routing table is correctly loaded on all routers. ● On Router D, verify that the IP address 192.168.2.2 can be pinged successfully.
A	A# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:40192.168.1.2 GigabitEthernet 0/1 192.168.2.2 1 Full/BDR00:00:34 192.168.2.2 GigabitEthernet 0/2 A# show ip route ospf O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

B	B# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.1.1 GigabitEthernet 0/1 192.168.3.2 1 Full/BDR00:00:30 192.168.3.2 GigabitEthernet 0/2 B# show ip route ospf O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
C	C# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.2.1 GigabitEthernet 0/3 C# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
D	D# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.21 Full/BDR00:00:30 192.168.3.1 GigabitEthernet 0/3 D# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3 D# ping 192.168.2.2 Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.

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 enabled on adjacent interfaces are inconsistent.
- The same router ID is configured on multiple routers, resulting in a router ID conflict.
- The same interface IP address is configured on multiple routers, resulting in a running error of the OSPF network.

2.4.2 Setting the Network Type

Configuration Effect

- Run OSPF to provide the IPv4 unicast routing service if the physical network is X.25, frame relay, or ATM.

Notes

- The OSPF basic functions must be configured.
- The broadcast network sends OSPF packets in multicast mode. Neighbors are automatically discovered, and the DR/BDR election is required.
- The P2P network sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The NBMA network sends OSPF packets in unicast mode. Neighbors must be manually specified, and the DR/BDR election is required.
- The P2MP network (without the **non-broadcast** parameter) sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The P2MP network (with the **non-broadcast** parameter) sends OSPF packets in unicast mode. Neighbors must be manually specified.

Configuration Steps

↘ **Configuring the Interface Network Type**

- Optional.
- The configuration is required on routers at both ends of the link.

↘ **Configuring Neighbors**

- (Optional) If the interface network type is set to NBMA or P2MP (with the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (with the **non-broadcast** parameter) network.

↘ **Configuring the Interface Priority**

- (Optional) 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.

Verification

- Run the **show ip ospf interface** command to verify that the network type of each interface is correct.

Related Commands

Configuring the Interface Network Type

Command	**ip ospf network** { **broadcast**| **non-broadcast**| **point-to-multipoint**[**non-broadcast**] | **point-to-point**}
Parameter Description	**broadcast**: Sets the interface network type to broadcast. **non-broadcast:** Sets the interface network type to non-broadcast. **point-to-multipoint** [**non-broadcast**]: Sets the interface network type to P2MP. If the interface does not have the broadcast capability, the **non-broadcast** parameter must be available. **point-to-point:** Sets the interface network type to P2P.
Command Mode	Interface configuration mode
Usage Guide	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. The P2MP type does not raise any requirement.

Configuring Neighbors

Command	**neighbor** *ip-address* [**poll-interval***seconds*] [**priority***priority*] [**cost** *cost*]
Parameter Description	*ip-address*: Indicates the IP address of the neighbor interface. **poll-interval***seconds***:** Indicates the neighbor polling interval. The unit is second. The value ranges from 0 to 2,147,483,647. This parameter is applicable only to the NBMA interface. **priority***priority*: Indicates the neighbor priority. The value ranges from 0 to 255. This parameter is applicable only to the NBMA interface. **cost***cost***:** Indicates the cost required to reach each neighbor. There is no default value. The value ranges from 0 to 65,535. This parameter is applicable only to the P2MP interface.
Command Mode	OSPF routing process configuration mode
Usage Guide	Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface. 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 death 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 the adjacency. The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must use this command to manually configure neighbors for the P2MP (non-broadcast) network. In addition, you can use the **cost** parameter to specify the cost to reach each

	neighbor on the P2MP network.

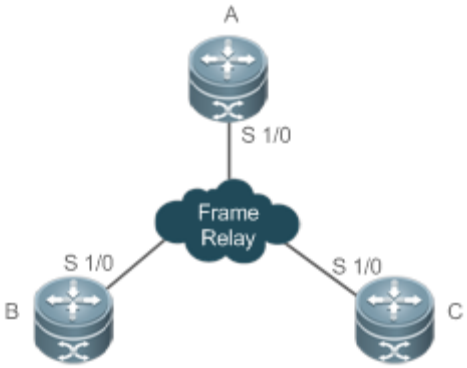
Configuring the Interface Priority

Command	**ip ospf priority** *priority*
Parameter Description	*priority*: Indicates the OSPF priority of an interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	The OSPF interface priority is contained in the Hello packet. 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. This command is applicable only to the OSPF broadcast and NBMA interfaces.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Setting the Interface Network Type to P2MP

Scenario **Figure 2-7**	 **Remarks**: The interface IP addresses are as follows: A: S1/0 192.168.1.2 B: S1/0 192.168.1.3 C: S1/0 192.168.1.4
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the interface network type to P2MP on all routers.

A	A#configure terminal A(config)# interface Serial1/0 A(config-Serial1/0)# encapsulation frame-relay A(config-Serial1/0)# ip ospf network point-to-multipoint
B	B#configure terminal B(config)# interface Serial1/0 B(config-Serial1/0)# encapsulation frame-relay B(config-Serial1/0)# ip ospf network point-to-multipoint
C	C#configure terminal C(config)# interface Serial1/0 C(config-Serial1/0)# encapsulation frame-relay C(config-Serial1/0)# ip ospf network point-to-multipoint
Verification	Verify that the interface network type is P2MP. A# show ip ospf interface Serial1/0 Serial1/0 is up, line protocol is up Internet Address 192.168.1.2/24, Ifindex 2, Area 0.0.0.1, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

Common Errors

- The network types configured on interfaces at two ends are inconsistent, causing abnormal route learning.
- The network type is set to NBMA or P2MP (with the **non-broadcast** parameter), but neighbors are not specified.

2.4.3 Configuring Route Redistribution and Default Route

Configuration Effect

- In the OSPF domain, introduce a unicast route to other AS domains so that the unicast routing service to other AS domains can be provided for users in the OSPF domain.
- In the OSPF domain, inject a default route to other AS domains so that the unicast routing service to other AS domains can be provided for users in the OSPF domain.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Configuring External Route Redistribution

- (Optional) This configuration is required if external routes of the OSPF domain should be introduced to an ASBR.
- This configuration is performed on an ASBR.

↘ Generating a Default Route

- (Optional) This configuration is required if the default route should be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.
- This configuration is performed on an ASBR.

Verification

- On a router inside the OSPF domain, run the **show ip route** command to verify that the unicast routes to other AS domains are loaded.
- On a router inside the OSPF domain, run the **show ip route** command to verify that the default route to the ASBR is loaded.
- Run the **ping** command to verify that the IPv4 unicast service to other AS domains is correct.

Related Commands

↘ Configuring External Route Redistribution

Command	**redistribute** { **connected** | **ospf** *process-id* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] | **rip** | **static** } [**metric** *metric-value*] [**metric-type** { **1** | **2** }] [**route-map** *route-map-name*] [**subnets**] [**tag***tag-value*]
Parameter Description	**connected:** Indicates redistribution from direct routes. **ospf** *process-id:* Indicates redistribution from OSPF. *process-id* specifies an OSPF process. The value ranges from 1 to 65,535. **rip:** Indicates redistribution from RIP. **static:** Indicates redistribution from static routes.

	match: Used only when OSPF routes are redistributed. Only the routes meeting the filtering conditions are redistributed. By default, all OSPF routes can be redistributed. **metric** *metric-value:* Specifies the metric of the OSPF external LSA. *metric-value* specifies the size of the metric. The value ranges from 0 to 16,777,214. **metric-type { 1 | 2 }**: Sets the external route type, which can be E-1 or E-2. **route-map** *route-map-name:* Sets the redistribution filtering rules. **subnets:** Specifies the non-standard networks for redistribution. **tag** *tag-value:* Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	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 use the **no** form of the command to restore the default value of **match**. For details, see the configuration example. If **route-map** is specified, the filtering rules specified in **route-map** are applicable to original parameters of redistribution. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

↘ Introducing a Default Route

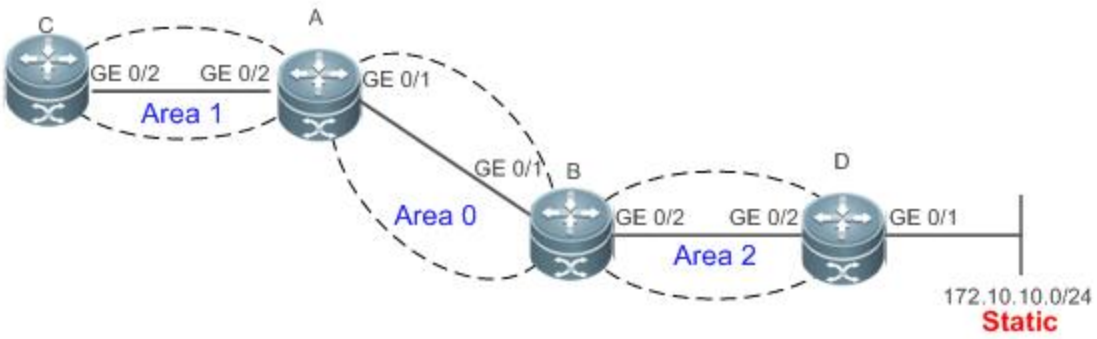
Command	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map-name*]
Parameter Description	**always:** Enables OSPF to generate a default route regardless of whether the local router has a default route. **metric** *metric:* Indicates the initial metric of the default route. The value ranges from 0 to 16,777,214. **metric-type***type:* Indicates the type of the default route. OSPF external routes are classified into two types: Type 1: The metric varies with routers; Type 2: The metric is the same for all routers. Type 1 external routes are more trustworthy than Type 2 external routes. **route-map** *map-name:* Indicates the associated route-map name. By default, no route-map is associated.
Command Mode	OSPF routing process configuration mode
Usage Guide	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 have the ASBR generates a default route, configure the **default-information originate** command.

	If **always** 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 link status database. 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. The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command. 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 have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ip route** command displays only the Type 1 route. A router in the stub area cannot generate an external default route. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced.

Configuration Example

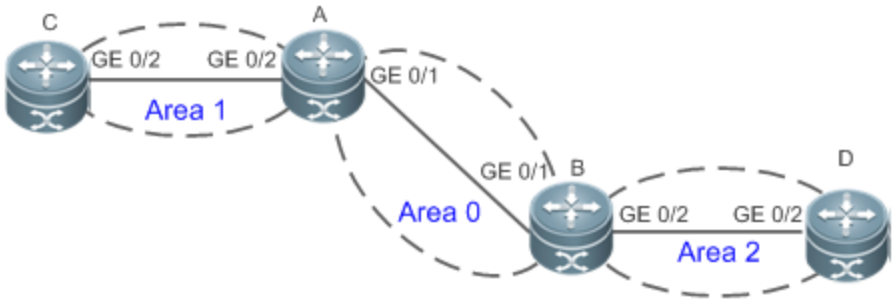
The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Configuring Static Route Redistribution

Scenario **Figure 2-8**	
Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D.

D	D# configure terminal D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.3 D(config)#router ospf 1 D(config-router)# redistribute staticsubnets
Verification	● On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to an external route is generated. ● On Router C, run the **show ip route ospf** command to verify that the external static route has been introduced.
D	D# show ip ospf database external brief OSPF Router with ID (192.168.22.30) (Process ID 1) AS External Link States Link ID ADV Router Age Seq# CkSum Route Tag 172.10.10.0 192.168.22.30 11 0x80000001 0xa4bb E2 172.10.10.0/24 0
C	C# show ip route ospf O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2

Configuring the Default Route

Scenario **Figure 2-9**	
	Remarks: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/2 192.168.3.2

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the default route on Router D.
D	D# configure terminal D(config)#router ospf 1 D(config-router)#default-information originate always
Verification	● On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to the default route is generated. ● On Router C, run the **show ip route ospf** command to verify that the OSPF default route exists.
D	D#show ip ospf database external brief OSPF Router with ID (192.168.22.30) (Process ID 1) AS External Link States Link ID ADV Router Age Seq# CkSum Route Tag 0.0.0.0 192.168.22.30 565 0x80000002 0xa190 E2 0.0.0.0/0 1
C	C# show ip route ospf O E20.0.0.0/0 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2

Common Errors

- The subnet route is not introduced because the **subnets** parameter in the **redistribute** command is not configured.
- A routing loop is formed because the **default-information originate always** command is configured on multiple routers.
- Routes cannot be introduced because route redistribution is configured on a router in the stub area.

2.4.4 Configuring Stub Area and NSSA Area

Configuration Effect

- 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.

Notes

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

Configuration Steps

Configuring a Stub Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area.
- The area must be configured as a stub area on all routers in this area.

Configuring an NSSA Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area and introduce OSPF external routes to the area.
- The area must be configured as an NSSA area on all routers in this area.

Verification

Verifying the Stub Area

- On a router in the stub area, run the **show ip route** command to verify that the router is not loaded with any external routes.

Verifying the NSSA Area

- On a router in the NSSA area, run the **show ip ospf database** command to verify that the introduced external route generates Type 7 LSAs.
- On a router in the backbone area, run the **show ip route** command to verify that the router is loaded with external routes introduced from the NSSA area.

Related Commands

Configuring a Stub Area

Command	**area** *area-id* **stub** [**no-summary**]
Parameter Description	*area-id:* Indicates the ID of the stub area. **no-summary:** Prohibits the ABR from sending network summary LSAs. At this time, the stub can be called totally stub area. This parameter is configured only when the router is an ABR.
Command Mode	OSPF routing process configuration mode
Usage Guide	You must run the **area stub** command on all routers in the OSPF stub area. The ABR sends only three types of LSAs to the stub area: (1) Type 1: Router LSA; (2) Type 2: Network LSA; (3) Type 3: Network Summary LSA. From the routing table point of view, a router in the stub area can learn only the internal routes of the OSPF routing domain, including the internal default route generated by an ABR. A router in the stub area cannot learn external routes of the OSPF routing domain. To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR. You can run either the **area stub** or **area default-cost** command to configure an OSPF area as a stub area.

	If **area stub** is used, you must configure this command on all routers connected to the stub area. If **area default-cost** is used, run this command only on the ABR in the stub area. The **area default-cost** command defines the initial cost (metric) of the internal default route.

Configuring an NSSA Area

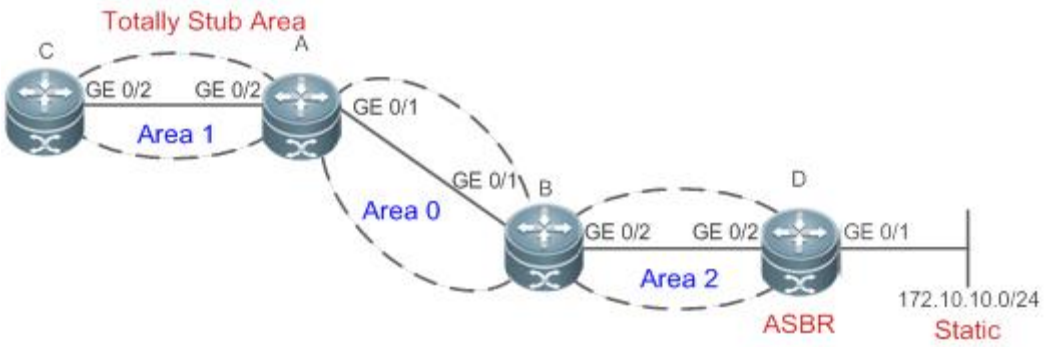
Command	**area***area-id* **nssa** [**no-redistribution**] [**default-information-originate**[**metric***value*] [**metric-type***type*]] [**no-summary**] [**translator** {**stability-interval***seconds* | **always**} **]**
Parameter Description	*area-id:* Indicates the ID of the NSSA area. **no-redistribution:** Select this option if the router is an NSSA ABR and you want to use only the **redistribute** command to introduce the routing information into a common area instead of an NSSA area. **default-information-originate:** Indicates that a default Type 7 LSA is generated and introduced to the NSSA area. This option takes effect only on an NSSA ABR or ASBR. **metric***value:* Specifies the metric of the generated default LSA. The value ranges from 0 to 16,777,214. The default value is 1. **metric-type***type:* Specifies the route type of the generated default LSA. The values include 1 and 2. **1** represents N-1, and **2** represents N-2. The default value is 2. **no-summary:** Prohibits the ABR in the NSSA area from sending summary LSAs (Type-3 LSA). **translator:** Indicates that the NSSA ABR is a translator. **stability-interval***seconds:* Indicates the stability interval after the NSSA ABR is changed from a translator to a non-translator. The unit is second. The default value is 40. The value ranges from 0 to 2,147,483,647. **always:** Indicates that the current NSSA ABR always acts as a translator. The default value is the standby translator.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA area. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table. If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be advertised to the NSSA area. This parameter is generally used when a router in the NSSA area acts both as the ASBR and the ABR. It prevents external routing information from entering the NSSA area. To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSA) to the NSSA area. **area default-cost** is used on an ABR or ASBR connected to the NSSA area. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1. If an NSSA area has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for converting Type 7 LSAs into Type 5 LSAs. If the current device is always the translator ABR for converting Type 7 LSAs into Type 5 LSAs, use the **translator always** parameter.

	If the translator role of the current device is replaced by another ABR, the conversion capability is retained during the time specified by **stability-interval**. If the router does not become a translator again during **stability-interval**, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires. To prevent a routing loop, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS immediately after the current device loses the translator role even if **stability-interval** does not expire. In the same NSSA area, it is recommended that **translator always** be configured on only one ABR.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Configuring a Stub Area

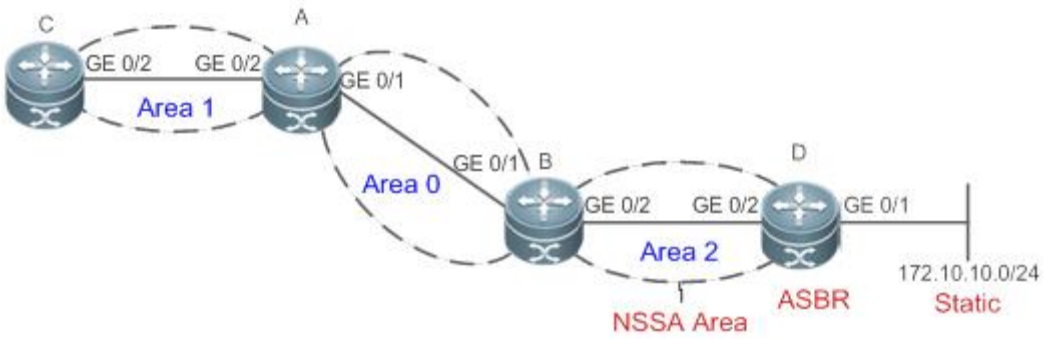
Scenario **Figure 2-10**	 **Remarks** The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 1 as the stub area on Router A and Router C.

D	`D# configure terminal`
	`D(config)#router ospf 1`
	`D(config-router)# redistribute staticsubnets`

A	`A# configure terminal`
	`A(config)#router ospf 1`
	`A(config-router)#area 1 stubno-summary`

C	C# configure terminal C(config)#router ospf 1 C(config-router)#area 1 stub
Verification	On Router 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 Router D.
	C#show ip route ospf O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2

Configuring an NSSA Area

Scenario **Figure 2-11**	
	Remarks: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 2 as the NSSA area on Router B and Router D.
B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 2 nssa
D	D# configure terminal D(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2 D(config)#router ospf 1

	D(config-router)#redistribute static subnets D(config-router)#area 2 nssa
Verification	● On Router D, verify that the Type 7 LSA, 172.10.10.0/24, is generated. ● On Router B, verify that Type 5 and Type 7 LSAs coexist on 172.10.10.0/24. ● On Router B, verify that the N-2 route of 172.10.10.0/24 is generated.
D	D# show ip ospf database nssa-external OSPF Router with ID (192.168.6.2) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 61 Options: 0x8 (-|-|-|-|N/P|-|-|-) LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001 Checksum: 0xc8f8 Length: 36 Network Mask: /24 Metric Type: 2 (Larger than any link state path) TOS: 0 Metric: 20 NSSA: Forward Address: 192.168.6.2 External Route Tag: 0
B	B# show ip ospf database nssa-external OSPF Router with ID (192.168.3.1) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 314 Options: 0x8 (-|-|-|-|N/P|-|-|-) LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001

```
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
B# show ip ospf database external
            OSPF Router with ID (192.168.3.1) (Process ID 1)
                AS External Link States
  LS age: 875
  Options: 0x2 (-|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 172.10.10.0 (External Network Number)
  Advertising Router: 192.168.3.1
  LS Seq Number: 80000001
  Checksum: 0xd0d3
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 192.168.6.2
        External Route Tag: 0


B# show ip route ospf
O N2  172.10.10.0/24 [110/20] via 192.168.3.2, 00:06:53, GigabitEthernet 0/2
```

Common Errors

- Configurations of the area type are inconsistent on routers in the same area.
- External routes cannot be introduced because route redistribution is configured on a router in the stub area.

2.4.5 Configuring Route Summarization

Configuration Effect

- Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.
- Shield or filter routes.

Notes

- The OSPF basic functions must be configured.
- 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 or shield or filter routes.

Configuration Steps

↘ Configuring Inter-Area Route Summarization

- (Optional) This configuration is required when routes of the OSPF area need to be summarized.
- Unless otherwise required, this configuration should be performed on an ABR in the area where routes to be summarized are located.

↘ Configuring External Route Summarization

- (Optional) This configuration is required when routes external to the OSPF domain need to be summarized.
- Unless otherwise required, this configuration should be performed on an ASBR to which routes to be summarized are introduced.

Verification

Run the **show ip route ospf** command to verify that individual routes do not exist and only the summarized route exists.

Related Commands

↘ Configuring Inter-Area Route Summarization

Command	**area** *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]
Parameter Description	*area-id*: Specifies the ID of the OSPF area to which the summarized route should be injected. The area ID can be a decimal integer or an IP address. *ip-address net-mask*: Defines the network segment of the summarized route. **advertise** | **not-advertise**: Specifies whether the summarized route should be advertised. **cost** *cost:* Indicates the metric of the summarized route. The value ranges from 0 to 16777215.
Command Mode	OSPF routing process configuration mode
Usage Guide	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 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. In addition, you can set **advertise** or **not-advertise** to determine whether to advertise the 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 route summarization commands for multiple areas. This simplifies routes in the entire OSPF routing domain, and improve the network forwarding performance, especially for a large-sized network. When multiple route summarization commands are configured and have the inclusive relationship with each other, the area range to be summarized is determined based on the maximum match principle.

Configuring External Route Summarization

Command	**summary-address** *ip-address net-mask* [**not-advertise** | **tag** *value*]
Parameter Description	*ip-address*: Indicates the IP address of the summarized route. *net-mask*: Indicates the subnet mask of the summarized route. **not-advertise**: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised. **tag***value:* Indicates the tag of the summarized route. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When routes are redistributed from other routing processes and injected to the OSPF routing process, each route is advertised to the OSPF routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertised only one summarized route to significantly reduce the size of the routing table. **area range** summarizes the routes between OSPF routes, 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.

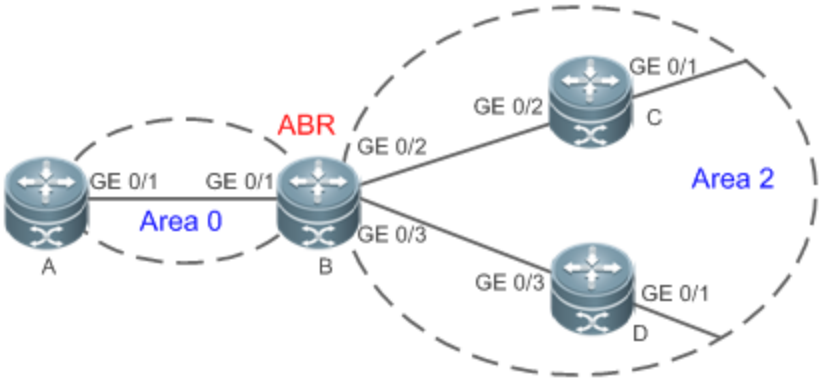
Configuring a Discard Route

Command	**discard-route** { **internal** | **external** }
Parameter Description	**internal:** Indicates that the discard route generated by the **area range** command can be added. **external:** Indicates that the discard route generated by the **summary-address** command can be added.
Command Mode	OSPF routing process configuration mode
Usage Guide	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.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario **Figure 2-12**	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/1 172.16.4.2 D: GE0/2 172.16.3.2 GE0/1 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Summarize routes of area 2 on Router B.
B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 2 range 172.16.0.0 255.255.0.0
Verification	On Router A, verify that the entry 172.16.0.0/16 is added to the routing table.
A	A#show ip route ospf O IA 172.16.0.0/16 [110/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

Common Errors

- Inter-area route summarization cannot be implemented because the **area range** command is configured on a non-ABR device.

2.4.6 Configuring Route Filtering

Configuration Effect

- 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.

Notes

- The OSPF basic functions must be configured.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, 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.

Configuration Steps

Configuring Inter-Area Route Filtering

- (Optional) This configuration is recommended if users should be restricted from accessing the network in a certain OSPF area.
- Unless otherwise required, this configuration should be performed on an ABR in the area where filtered routes are located.

Configuring Redistributed Route Filtering

- (Optional) This configuration is required if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, this configuration should be performed on an ASBR to which filtered routes are introduced.

Configuring Learned Route Filtering

- (Optional) This configuration is required if users should be restricted from accessing a specified destination network.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route** command to verify that the router is not loaded with routes that have been filtered out.
- Run the **ping** command to verify that the specified destination network cannot be accessed.

Related Commands

Configuring a Passive Interface

Command	**passive-interface**{ **default** | *interface-type interface-number* | *interface-type interface-numberip-address*}
Parameter Description	*interface-type interface-number*: Indicates the interface that should be configured as a passive interface. **default:** Indicates that all interface will be configured as passive interfaces. *interface-type interface-numberip-address:* Specifies an address of the interface as the passive address.
Command Mode	OSPF routing process configuration mode

Usage Guide	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.

Configuring the LSA Update Packet Filtering

Command	**ip ospf database-filter all out**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable this function on an interface to prevent sending the LSA update packet on this interface. After this function is enabled, the local router does not advertise the LSA update packet to neighbors, but still sets up the adjacency with neighbors and receives LSAs from neighbors.

Configuring Inter-Area Route Filtering

Command	**area** *area-id* **filter-list** {**access** *acl-name* | **prefix** *prefix-name*} {**in** | **out**}
Parameter Description	*area-id*: Indicates the area ID. **access** *acl-name*: Indicates the associated ACL. **prefix** *prefix-name*: Indicates the associated prefix list. **in** | **out:** Filters routes that are received by or sent from the area.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be configured only on an ABR. Use this command when it is required to configure filtering conditions for inter-area routes on the ABR.

Configuring Redistributed Route Filtering

Command	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**connected**] **| ospf** *process-id* **| static**]
Parameter Description	*access-list-number* | *name*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefix list for filtering. **connected** | **ospf** *process-id* | **static**: Indicates the source of routes to be filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	**distribute-list out** is similar to **redistribute route-map**, and is used to filter routes that are redistributed from other protocols to OSPF. The **distribute-list out** command itself does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and the prefix list filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes coming from a certain source, the prefix list cannot be configured to filter the same routes.

Configuring Learned Route Filtering

Command	**distribute-list** {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map**

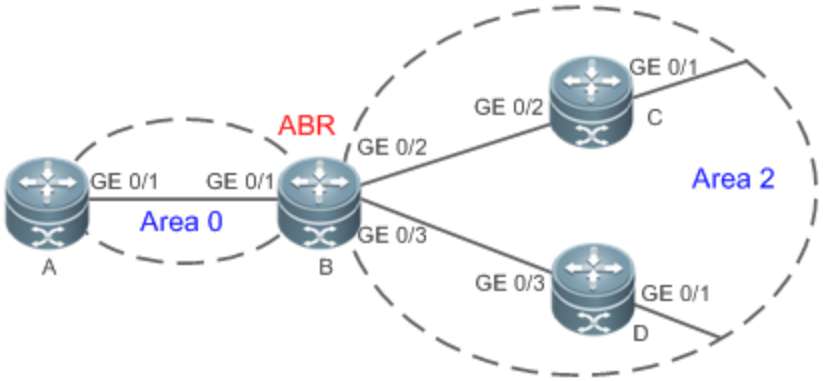
	route-map-name } **in** [*interface-typeinterface-number*]
Parameter Description	*access-list-number*	*name*: Uses the ACL for filtering. **gateway***prefix-list-name*: Uses the gateway for filtering. **prefix***prefix-list-name*: Uses the prefixlist for filtering. **route-map** *route-map-name:* Uses the route map for filtering. *interface-type interface-number:* Specifies the interface for which LSA routes are filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	Filter routes that are computed based on received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL, prefix list, and route map filtering rules are mutuallyexclusive in the configuration. That is, if the ACL is used for filtering routes of a specified interface, the prefix list or router map cannot be configured for filtering routes of the same interface.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario	

Figure 2-13



Remarks	The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure route filtering.
A	A# configure terminal A(config)#access-list 3 permit host 172.16.5.0 A(config)#router ospf 1 A(config-router)#distribute-list 3 in GigabitEthernet 0/1

Verification	● On Router A, check the routing table. Verify that only the entry 172.16.5.0/24 is loaded.
A	A# show ip route ospf O 172.16.5.0/24 [110/2] via 192.168.1.2, 10:39:40, GigabitEthernet 0/1

Common Errors

- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, 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.

2.4.7 Modifying Route Cost and AD

Configuration Effect

- Change the OSPF routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

Notes

- 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.

Configuration Steps

↘ Configuring the Reference Bandwidth

- Optional.
- A router is connected with lines with different bandwidths. This configuration is recommended if you wish to preferentially select the line with a larger bandwidth.

↘ Configuring the Cost of an Interface

- Optional.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.

↘ Configuring the Default Metric for Redistribution

- Optional.
- 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.

Configuring the Maximum Metric

- Optional.
- A router may be unstable during the restart process or a period of time after the router is restarted, and users do not want to forward data through this router. In this case, this configuration is recommended.

Configuring the AD

- Optional.
- This configuration is mandatory if you wish to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.

Verification

- Run the **show ip ospf interface** command to verify that the costs of interfaces are correct.
- Run the **show ip route** command to verify that the costs of external routes introduced to the ASBR are correct.
- Restart the router. Within a specified period of time, data is not forwarded through the restarted router.

Related Commands

Configuring the Reference Bandwidth

Command	**auto-costreference-bandwidth** *ref-bw*
Parameter Description	*ref-bw*: Indicates the reference bandwidth. The unit is Mbps. The value ranges from 1 to 4,294,967.
Command Mode	OSPF routing process configuration mode
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps 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.

Configuring the Cost of an Interface

Command	**ip ospf cost***cost*
Parameter Description	*cost*: Indicates the cost of an OSPF interface. The value ranges from 0 to 65,535.
Command	Interface configuration mode

Mode	
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps 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.

Configuring the Cost of the Default Route in a Stub or an NSSA Area

Command	**area***area-id* **default-cost***cost*
Parameter Description	*area-id*: Indicates the ID of the stub or NSSA area. *cost*: Indicates the cost of the default summarized route injected to the stub or NSSA area. The value ranges from 0 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR in a stub area or an ABR/ASBR in an NSSA area. An ABR in a stub area or an ABR/ASBR in an NSSA area is allowed to advertise an LSA indicating the default route in the stub or NSSA area. You can run the **area default-cost** command to modify the cost of the advertised LSA.

Configuring the Default Metric for Redistribution

Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric of the OSPF redistributed route. The value ranges from 1 to 16,777,214.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-metric** command must be used together with the **redistribute** command 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 by the **default-information originate** command.

Configuring the Maximum Metric

Command	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup**[*seconds*]] [**summary-lsa** [*max-metric-value*]]
Parameter Description	**router-lsa**: Sets the metrics of non-stub links in the Router LSA to the maximum value (0xFFFF). **external-lsa**: Allows a router to replace the metrics of external LSAs (including Type 5 and Type 7 LSAs)

	with the maximum metric. *max-metric-value*: Indicates the maximum metric of the LSA. The default value is 16711680. The value ranges from 1 to 16,777,215. **include-stub:** Sets the metrics of stub links in the Router LSA advertised by the router to the maximum value. **on-startup:** Allows a router to advertises the maximum metric when started. *seconds:* Indicates the interval at which the maximum metric is advertised. The default value is 600s. The value ranges from 5 to 86,400. **summary-lsa:** Allows a router to replace the metrics of summary LSAs (including Type 3 and Type 4 LSAs) with the maximum metric.
Command Mode	OSPF routing process configuration mode
Usage Guide	After the **max-metric router-lsa** command is executed, 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 executed, 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 does not wish to transfer inter-area traffic, use the **summary-lsa** parameter to set the metric of the Summary LSA to the maximum metric. 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 metric. The **max-metric router-lsa** command is generally used in the following scenarios: Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. ● 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 executed, the current device advertises the maximum metric among all metrics of routes. In this way, other devices on the network can select the standby 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.

Configuring RFC1583Compatibility

Command	**compatible rfc1583**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode

Usage Guide	When there are multiple paths to an ASBR or the forwarding address of an external route, RFC1583 and RFC2328 define different routing rules. If RFC1583 compatibility is configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC1583 compatibility is not configured, a path in a non-backbone area is preferentially selected.

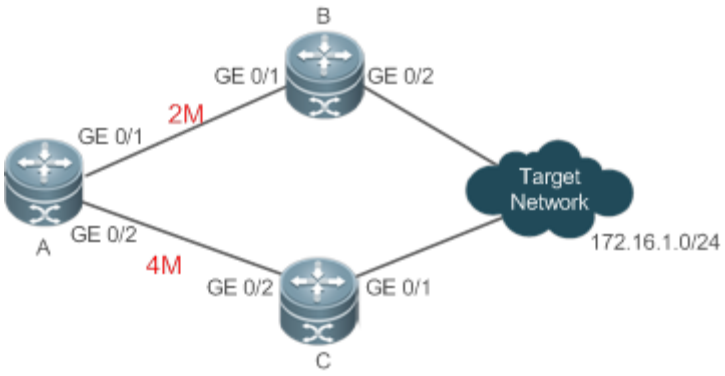
Configuring the AD

Command	**distance** { *distance* | **ospf** { [**intra-area***distance*] [**inter-area***distance*][**external** *distance*]} }
Parameter Description	*distance*: Indicates the AD of a route. The value ranges from 1 to 255. **intra-area** *distance*: Indicates the AD of an intra-area route. The value ranges from 1 to 255. **inter-area** *distance*: Indicates the AD of an inter-area route. The value ranges from 1 to 255. **external** *distance:* Indicates the AD of an external route. The value ranges from 1 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	Use this command to specify different ADs for different types of OSPF routes.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Configuring the Cost of an Interface

Scenario **Figure 2-14**	
Remarks	The interface IP addresses are as follows: A: GE0/1 192.168.1.1 GE0/2 192.168.2.1 B: GE0/1 192.168.1.2 GE0/2 192.168.3.2 C: GE0/1 192.168.4.2 GE0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure the cost of each interface.

A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf cost 10 A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip ospf cost 20
Verification	On Router A, check the routing table. The next hop of the optimum path to 172.16.1.0/24 is Router B.
A	A# show ip route ospf O E2172.16.1.0/0 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- If the cost of an interface is set to 0 in the **ip ospf cost** command, a route computation error may occur. For example, a routing loop is obtained.

2.4.8 Enabling Authentication

Configuration Effect

- All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

Notes

- 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.

Configuration Steps

↘ Configuring the Authentication Type of an Area

- (Optional) This configuration is recommended if the same authentication type should be used on all interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

↘ Configuring the Authentication Type of an Interface

- (Optional) This configuration is recommended if the different authentication types should be used on different interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

Configuring a Plain Text Authentication Key for an Interface

- Optional.
- This configuration is required if a router accesses a network that requires plain text authentication.

Configuring an MD5 Authentication Key for an Interface

- (Optional) MD5 authentication features a high security, and therefore is recommended. You must configure either plain text authentication or MD5 authentication.
- This configuration is required if a router accesses a network that requires MD5 authentication.

Verification

- If routers are configured with different authentication keys, run the **show ip ospf neighbor** command to verify that there is no OSPF neighbor.
- If routers are configured with the same authentication key, run the **show ip ospf neighbor** command to verify that there are OSPF neighbors.

Related Commands

Configuring the Authentication Type of an Area

Command	**area** *area-id* **authentication** [**message-digest**]
Parameter Description	*area-id*: Indicates the ID of the area where OSPF authentication is enabled. The area ID can be a decimal integer or an IP address. **message-digest**: Enables MD5 authentication.
Command Mode	OSPF routing process configuration mode
Usage Guide	The system supports three authentication types: (1) Type 0: No authentication is required. If this command is not configured to enable OSPF authentication, the authentication type in the OSPF data packet is 0. (2) Type 1: The authentication type is plain text authentication if this command is configured but does not contain the **message-digest** parameter. (3) Type 3: 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. You can run the interface configuration command **ip ospf authentication-key** to configure the plain text authentication key, or **ip ospf message-digest-key** to configure the MD5 authentication key.

Configuring the Authentication Type of an Interface

Command	**ip ospf authentication** [**message-digest** | **null**]
Parameter Description	**message-digest**: Indicates that MD5 authentication is enabled on the current interface. **null**: Indicates that authentication is disabled.

Command Mode	Interface configuration mode
Usage Guide	If the **ip ospfauthentication** command does not contain any option, it indicates that plain text authentication is enabled. If you use the **no** form of the command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to null, authentication is disabled forcibly. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

Configuring a Plain Text Authentication Key for an Interface

Command	**ip ospf authentication-key**[**0** |**7**]*key*
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key*: Indicates the key. The key is a string of up to eight characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf authentication-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. You can enable or disable authentication in an OSPF area by running the **areaauthentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. 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.

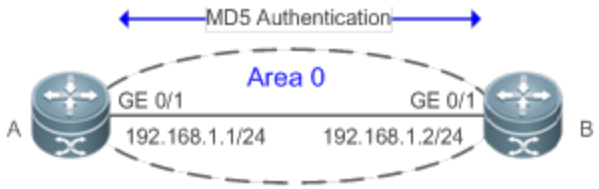
Configuring an MD5 Authentication Key for an Interface

Command	**ip ospf message-digest-key** *key-id* **md5**[**0** |**7**]*key*
Parameter Description	*key-id:* Indicates the key ID. The value ranges from 1 to 255. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key:* Indicates the key. The key is a string of up to 16 characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf message-digest-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. The same key ID on neighbor routers must

	correspond to the same key. You can enable or disable authentication in an OSPF area by running the **area authentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. 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. The system supports smooth modification of the MD5 authentication key. A new MD5 authentication key must be first added before the old key can be deleted. When an OSPF MD5 authentication key is added to a router, the router determines that other routers do not use the new key yet and therefore uses different keys to send multiple OSPF packets until it confirms that the new key has been configured on neighbors. After configuring the new key all routers, you can delete the old key.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario **Figure 2-15**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.
A	A# configure terminal A(config)#router ospf 1 A(config-router)#area 0 authentication message-digest A(config-router)#exit A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5 hello

B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 0 authentication message-digest B(config-router)#exit B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5 hello
Verification	On Router A and Router B, verify that the OSPF neighbor status is correct.
A	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:32 192.168.1.2 GigabitEthernet 0/1
B	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/DR 00:00:32 192.168.1.1 GigabitEthernet 0/1

Common Errors

- The authentication modes configured on routers are inconsistent.
- The authentication keys configured on routers are inconsistent.

2.4.9 Enabling Overflow

Configuration Effect

- New routes are not loaded to routers when the router memory is insufficient.
- New routes are not loaded to routers when the usage of the database space reaches the upper limit.

Notes

- 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 to exit the overflow state.

Configuration Steps

↘ **Configuring the Memory Overflow Function**

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the Database Overflow Function

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the External LSA Database Overflow Function

- Optional.
- This configuration is recommended if the ASBR introduces a large number of external routes and the router memory may be insufficient.

Verification

- After the memory becomes insufficient, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.
- After the usage of the database space reaches the upper limit, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.

Related Commands

Configuring the Memory Overflow Function

Command	**overflow memory-lack**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively ensure that the memory usage does not increase. 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 use 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.

Configuring the Database Overflow Function

Command	**overflow database***number* [**hard	soft**]
Parameter Description	*number*: Indicates the maximum number of LSAs. The value ranges from 1 to 4,294,967,294. **hard**: Indicates that the OSPF process will be stopped if the number of LSAs exceeds the limit. **soft:** Indicates that a warning will be generated if the number of LSAs exceeds the limit.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs exceeds the limit, use the **hard** parameter if the OSPF process should be stopped, and use the **soft** parameter if a warning should be generated without stopping the OSPF process.

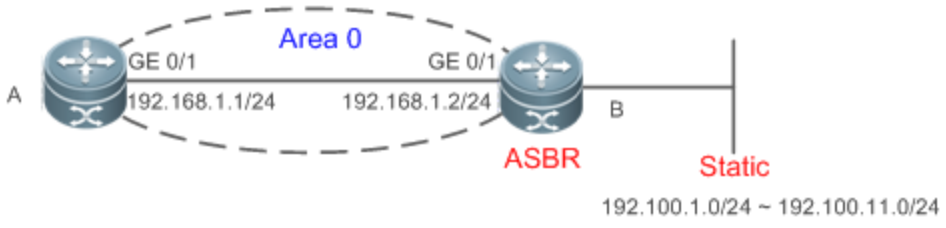
Configuring the External LSA Database Overflow Function

Command	**overflow database external** *max-dbsize wait-time*
Parameter Description	*max-dbsize*: Indicates the maximum number of external LSAs. This value must be the same on all routers in the same AS. The value ranges from 0 to 2,147,483,647. *wait-time*: Indicates the waiting time after a router in overflow state attempts to restore the normal state. The value ranges from 0 to 2,147,483,647.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the number of external LSAs of a router exceeds the configured **max-dbsize**, the router enters the overflow state. In this state, the router no longer loads external LSAs and deletes external LSAs that are generated locally. After *wait-time* elapses, the device restores the normal state, and loads external LSAs again. 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: Inconsistent LSDBs throughout network are inconsistent, and the failure to achieve the full adjacency Incorrect routes, including routing loops Frequent retransmission of AS external LSAs

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Configuring the External LSA Database Overflow Function

Scenario **Figure 2-16**	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router B, configure redistribution and introduce external static routes. ● On Router B, configure the maximum number of external LSAs.
B	B# configure terminal B(config)# router ospf 1 B(config-router)# redistribute static subnets
A	A# configure terminal A(config)# router ospf 1 A(config-router)# overflow database external 10 3
Verification	On Router B, configure 11 static routes (192.100.1.0/24 to 192.100.11.0/24). On Router A, verify that only 10 static routes are loaded.
A	A# show ip route ospf O E2 192.100.1.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.2.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.3.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.4.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.5.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.6.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.7.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.8.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.9.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.10.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- The OSPF adjacency is abnormal because the maximum number of LSAs is inconsistent on different routers.

2.4.10 Modifying the Maximum Number of Concurrent Neighbors

Configuration Effect

- Control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

- (Optional) This configuration is recommended if you wish to set up the OSPF adjacency more quickly when a router is connected with a lot of other routers.
- This configuration is performed on a core router.

Verification

- Run the **show ip ospf neighbor** command to display the number of neighbors that are concurrently interacting with the OSPF process.

Related Commands

Configuring the Maximum Number of Concurrent Neighbors on the Current Process

Command	**max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	OSPF routing process configuration mode
Usage Guide	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 one OSPF process can concurrently initiates or accepts interaction.

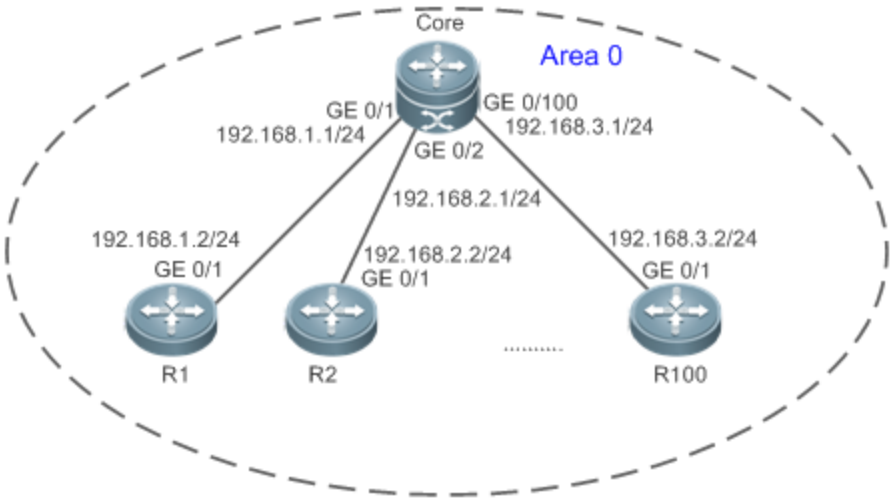
Configuring the Maximum Number of Concurrent Neighbors on All Processes

Command	**router ospf max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	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.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

Scenario **Figure 2-17**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On the router Core, set the maximum number of concurrent neighbors to 4.
Core	`Core# configure terminal` `Core(config)# router ospf max-concurrent-dd 4`
Verification	On the router Core, check the neighbor status and verify that at most eight neighbors concurrently interact with the OSPF process.

2.4.11 Disabling Source Address Verification

Configuration Effect

- The unicast routing service can be provided even if the interface IP addresses of neighbor routers are not in the same network segment.

Notes

- The OSPF basic functions must be configured.
- Source address verification cannot be disabled on a broadcast or NBMA network.

Configuration Steps

↘ Disabling Source Address Verification

- (Optional) This configuration is mandatory if an adjacency should be set up between routers with interface IP addresses in different network segments.
- This configuration is performed on routers with interface IP addresses in different network segments.

Verification

- An adjacency can be set up between routers in different network segments.

Related Commands

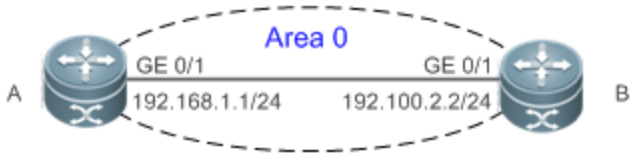
Disabling Source Address Verification

Command	ip ospf source-check-ignore
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	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 does not verify the address of an unnumbered interface. In some scenarios, the source address may not meet the preceding requirement, and therefore 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.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Disabling Source Address Verification

Scenario	
Figure 2-18	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the network types of interfaces on all routers to P2P. ● Disable source address verification on all routers.

A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point A(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point B(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
Verification	On Router A, verify that the OSPF neighbor information is correct.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.100.2.2 1 Full/- 00:00:34 192.100.2.2 GigabitEthernet 0/1

2.4.12 Disabling MTU Verification

Configuration Effect

- The unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Disabling MTU Verification

- (Optional) MTU verification is disabled by default. You are advised to retain the default configuration.
- This configuration is performed on two routers with different interface MTUs.

Verification

The adjacency can be set up between routers with different MTUs.

Related Commands

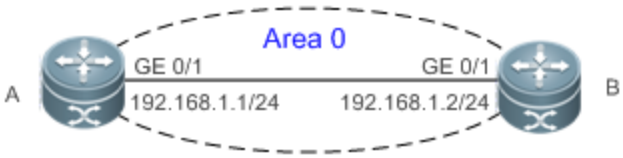
↘ Disabling MTU Verification

Command	**ip ospf mtu-ignore**
Parameter	N/A

Description	
Command Mode	Interface configuration mode
Usage Guide	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.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario Figure 2-19	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure different MTUs for interfaces on two routers. ● Disable MTU verification on all routers. (By default, the function of disabling MTU verification is enabled.)

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip mtu 1400`
	`A(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore`

B	`B# configure terminal`
	`B(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip mtu 1600`
	`B(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore`

Verification	● On Router A, verify that the OSPF neighbor information is correct.

A	`A# show ip ospfneighbor`
	`OSPF process 1, 1 Neighbors, 1 is Full:`
	`Neighbor ID Pri State Dead Time Address Interface`
	`192.168.1.2 1 Full/DR 00:00:34 192.168.1.2 GigabitEthernet 0/1`

2.4.13 Enabling Two-Way Maintenance

Configuration Effect

- Non-Hello packets can also be used to maintain the adjacency.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Enabling Two-Way Maintenance

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Non-Hello packets can also be used to maintain the adjacency.

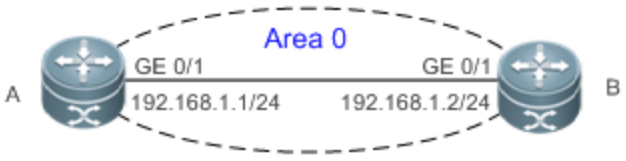
Related Commands

Enabling Two-Way Maintenance

Command	two-way-maintain
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	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 processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed due to timeout. 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 when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded Hello packets.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario Figure 2-20	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, enable the two-way maintenance function. (This function is enabled by default.)
A	A# configure terminal A(config)#routerospf 1 A(config-router)#two-way-maintain
Verification	When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/BDR 00:00:40 192.168.1.2 GigabitEthernet 0/1

2.4.14 Enabling GR

Configuration Effect

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Notes

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper function.
- The grace period cannot be shorter than the neighbor dead time of the neighbor router.

Configuration Steps

↘ Configuring the OSPF GR Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

↘ Configuring the OSPF GR Helper Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Related Commands

Configuring the OSPF GR Function

Command	**graceful-restart** [**grace-period** *grace-period* | **inconsistent-lsa-checking**]
Parameter Description	**grace-period** *grace-period*: Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s. **inconsistent-lsa-checking**: Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence. After GR is enabled, topological change detection is enabled by default.
Command Mode	OSPF routing process configuration mode
Usage Guide	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 status is rebuilt so that the original state of the OSPF process is restored. After the grace period expires, OSPF exits the GR state and performs common OSPF operations. Run the **graceful-restart** command to set the grace period to 120s. The **graceful-restart grace-period** command allows you to modify the grace period explicitly. The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole. Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time. Enabling topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled. In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process. If the Fast Hello function is enabled, the GR function cannot be enabled.

Configuring the OSPF GR Helper Function

Command	**graceful-restart helper** { **disable | strict-lsa-checking | internal-lsa-checking**}
Parameter Description	**disable**: Prohibits a device from acting as a GR helper for another device. **strict-lsa-checking**: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network

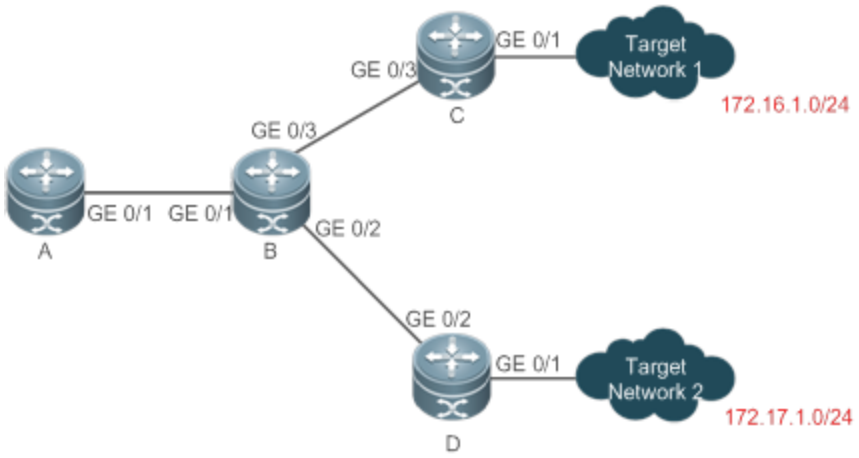
	changes, the device will stop acting as the GR helper. **internal-lsa-checking:** Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR. After a device becomes the 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 wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 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.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario

Figure 2-21



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1 C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2 D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, Router C, and Router D, enable the GR helper function. (This function is enabled by default.) ● On Router B, enable the GR function.
B	B# configure terminal B(config)# router ospf1 B(config-router)# graceful-restart
Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination networks 1 and 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination network 1 from Router A, and verify that data forwarding is not interrupted during the switchover.

Common Errors

- Traffic forwarding is interrupted during the GR process because the configured grace period is shorter than the neighbor dead time of the neighbor router.

2.4.15 Configuring the Network Management Function

Configuration Effect

- Use the network management software to manage OSPF parameters and monitor the OSPF running status.

Notes

- 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.

Configuration Steps

↘ Binding the MIB with the OSPF Process

- (Optional) This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.
- This configuration is performed on all routers.

↘ Enabling the Trap Function

- (Optional) This configuration is required if you want to use the network management software to monitor the OSPF running status.

- This configuration is performed on all routers.

Configuring the Logging Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration. If you want to reduce the log output, disable this function.
- This configuration is performed on all routers.

Verification

- Use the network management software to manage the OSPF parameters.
- Use the network management software to monitor the OSPF running status.

Related Commands

Binding the MIB with the OSPF Process

Command	**enable mib-binding**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	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 wish to perform operations on a specified OSPFv2 through SNMP, run this command to bind the MIB with the process.

Enabling the Trap Function

Command	**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**]]
Parameter Description	**IfAuthFailure**: Indicates that an interface authentication failure occurs. **IfConfigError:** Indicates that an interface parameter configuration error occurs. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **VirtIfAuthFailure:** Indicates that a virtual interface authentication failure occurs. **VirtIfConfigError:** Indicates that a virtual interface parameter configuration error occurs. **VirtIfRxBadPacket:** Indicates that the virtual interface receives a bad packet. **LsdbApproachOverflow:** Indicates that the number of external LSAs has reached 90% of the upper limit. **LsdbOverflow:** Indicates that the number of external LSAs has reached the upper limit.

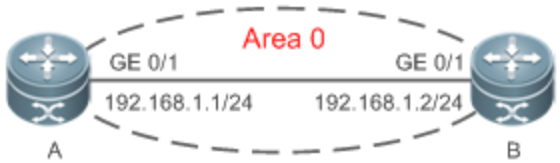
	MaxAgeLsa: Indicates that the LSA aging timer expires. **OriginateLsa:** Indicates that a new LSA is generated. **IfTxRetransmit:** Indicates that a packet is retransmitted on the interface. **VirtIfTxRetransmit:** Indicates that a packet is retransmitted on the virtual interface. **IfStateChange:** Indicates that interface state changes. **NbrRestartHelperStatusChange:**Indicates that the state of the neighbor GR process changes. **NbrStateChange:** Indicates that the neighbor state changes. **NssaTranslatorStatusChange:** Indicates that the NSSA translation state changes. **RestartStatusChange:** Indicates that the GR state of the local device changes. **VirtIfStateChange:** Indicates that the virtual interface state changes. **VirtNbrRestartHelperStatusChange:** Indicates that the GR state of the virtual neighbor changes. **VirtNbrStateChange:** Indicates that the virtual neighbor state changes.
Command Mode	OSPF routing process configuration mode
Usage Guide	The function configured by this command is restricted by the **snmp-server** command. You can configure **snmp-server enable traps ospf** and then **enable traps** command before the corresponding OSPF traps can be correctly sent out. This command is not restricted by the MIB bound with the process. The trap function can be enabled concurrently for different processes.

Configuring the Logging Function

Command	**log-adj-changes**[**detail**]
Parameter Description	**detail**: Records all status change information.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Scenario **Figure 2-22**	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Bind the MIB with the OSPF process on Router A. ● Enable the trap function on Router A.
A	A# configure terminal A(config)# snmp-server host 192.168.2.2 traps version 2c public A(config)# snmp-server community public rw A(config)# snmp-server enable traps A(config)# router ospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps
Verification	Use the MIB tool to read and set the OSPF parameters and display the OSPF running status.

Common Errors

Configurations on the SNMP-Server are incorrect. For example, the MIB or trap function is not enabled.

2.4.16 Modifying Protocol Control Parameters

Configuration Effect

Modify protocol control parameters to change the protocol running status.

Notes

- The OSPF basic functions must be configured.
- The neighbor dead time cannot be shorter than the Hello interval.

Configuration Steps

↘ Configuring the Hello Interval

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on routers at both end of a link.

↘ Configuring the Dead Interval

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails.
- This configuration is performed on routers at both end of a link.

↘ Configuring LSU Retransmission Interval

- (Optional) You are advised to adjust this configuration if a lot of routes exist in the user environment and network congestion is serious.

Configuring the LSA Generation Time

- (Optional) You are advised to retain the default configuration.

Configuring the LSA Group Refresh Time

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if a lot of routes exist in the user environment.
- This configuration is performed on an ASBR or ABR.

Configuring LSA Repeated Receiving Delay

- (Optional) You are advised to retain the default configuration.

Configuring the SPF Computation Delay

- (Optional) This configuration can be adjusted if network flapping frequently occurs.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Configuring the External Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Run the **show ip ospf** and **show ip ospf neighbor** commands to display the protocol running parameters and status.

Related Commands

Configuring the Hello Interval

Command	**ip ospf hello-interval***seconds*
Parameter Description	*seconds*: Indicates the interval at which OSPF sends the Hello packet. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The Hello interval is contained in the Hello packet. A shorter Hello interval indicates that OSPF can detect topological changes more quickly, but the network traffic increases. The Hello 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 interval.

Configuring the Dead Interval

Command	**ip ospf dead-interval** *seconds*
Parameter Description	*seconds*: Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647.
Command Mode	Interface configuration mode
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment.

Configuring the LSU Transmission Delay

Command	**ip ospf transmit-delay***seconds*
Parameter Description	*seconds*: Indicates the LSU transmission delay on the OSPF interface. The unit is second. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	Before an LSU packet is transmitted, the Age fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmit and line propagation delays on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU 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 will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Configuring LSU Retransmission Interval

Command	**ip ospf retransmit-interval***seconds*
Parameter Description	*seconds*: Indicates the LSU retransmission interval. The unit is second. The value ranges from 1 to 65,535. This interval must be longer than the round-trip transmission delay of data packets between two neighbors.
Command Mode	Interface configuration mode
Usage Guide	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 time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unnecessary retransmission. The LSU retransmission delay of a virtual link is defined by the **retransmit-interval** parameter in the **area virtual-link** command.

Configuring the LSA Generation Time

Command	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Parameter Description	*delay-time*: Indicates the minimum delay for LSA generation. The first LSA in the database is always generated instantly. The value ranges from 0 to 600,000. The unit is ms. *hold-time*: Indicates the minimum interval between the first LSA update and the second LSA update. The value ranges from 1 to 600,000. The unit is ms. *max-wait-time*: Indicates the maximum interval between two LSA updates when the LSA is updated continuously. This interval is also used to determine whether the LSA is updated continuously. The value ranges from 1 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	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 values of the preceding parameters to reduce the CPU usage. When configuring this command, the value of **hold-time** cannot be smaller than the value of **delay-time,** and the value of **max-wait-time** cannot be smaller than the value of **hold-time**.

Configuring the LSA Group Refresh Time

Command	**timers pacing lsa-group** *seconds*
Parameter Description	*seconds*: Indicates the LSA group pacing interval. The value ranges from 10 to 1,800. The unit is second.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every LSA has a time to live (LSA 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. In order 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 processes 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 1000 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.

Configuring the LSA Group Refresh Interval

Command	**timers pacing lsa-transmit** *transmit-time transmit-count*
Parameter Description	*transmit-time*: Indicates the LSA group transmission interval. The value ranges from 10 to 1,000. The unit is ms. *transmit-count*: Indicates the number of LS-UPD packets in a group. The value ranges from 1 to 200.
Command	OSPF routing process configuration mode

Mode	
Usage Guide	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 a 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.

Configuring LSA Repeated Receiving Delay

Command	**timers lsa arrival** *arrival-time*
Parameter Description	*arrival-time*: Indicates the delay after which the same LSA is received. The value ranges from 0 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	No processing is performed if the same LSA is received within the specified time.

Configuring the Inter-Area Route Computation Delay

Command	**timers throttle route inter-area** *ia-delay*
Parameter Description	*ia-delay*: Indicates the inter-area route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the External Route Computation Delay

Command	**timers throttle route ase** *ase-delay*
Parameter Description	*ase-delay*: Indicates the external route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the SPF Computation Delay

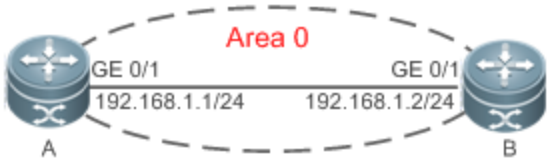
Command	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Parameter Description	*spf-delay*: Indicates the SPF computation delay. The unit is ms. The value ranges from 1 to 600,000. When detecting a topological change, the OSPF routing process triggers the SPF computation at least after **spf-delay** elapses. *spf-holdtime*: Indicates the minimum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *spf-max-waittime*: Indicates the maximum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *number*: indicates the metric of the summarized route.

Command Mode	OSPF routing process configuration mode
Usage Guide	**spf-delay** indicates the minimum time between the occurrence of the topological change and the start of SPF computation. **spf-holdtime** indicates the minimum interval between the first SPF computation and the second SPF computation. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches **spf-max-waittime**, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval is computed by starting from **spf-holdtime**. You can set **spf-dela**y and **spf-holdtime** to smaller values to accelerate topology convergence, and set **spf-max-waittime** to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology. Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration. 1. The value of **spf-holdtime** cannot be smaller than the value of **spf-delay**; otherwise, **spf-holdtime** will be automatically set to the value of **spf-delay**. 2. The value of **spf-max-waittime** cannot be smaller than the value of **spf-holdtime**; otherwise, **spf-max-waittime** will be automatically set to the value of **spf-holdtime**. 3. The configurations of **timers throttle spf** and **timers spf** are mutually overwritten. 4. When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 2.4.1 "Configuring OSPF Basic Functions."

Configuring the Hello Interval and Dead Interval

Scenario **Figure 2-23**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the Hello interval and dead interval on all routers.

A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
Verification	Check the interface parameters on Router A. Verify that the Hello interval is 10s and the dead interval is 50s.
A	A# show ip ospf interface GigabitEthernet 0/1 is up, line protocol is up Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 15, Dead 50, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

Common Errors

- The configured neighbor dead time is shorter than the Hello interval.

2.5 Monitoring

Clearing

⚠ Running the **clear** commands maylose vital information and thus interrupt services.

Description	Command

Clears and resets an OSPF process.	**clear ip ospf** [*process-id*] **process**

Displaying

Description	Command
Displays the OSPF process configurations.	**show ip ospf** [*process-id*]
Displays the OSPF internal routing table, including routes to ABRs and ASBRs.	**show ip ospf**[*process-id*] **border-routers**
Displays information about the OSPF LSDB.	**show ip ospf** [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }][{ **adv-router** *ip-address*| **self-originate** } |*link-state-id* | **brief**][**database-summary** | **max-age** | **detail**]
Displays OSPF-enabled interfaces.	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
Displays the OSPF neighbor list.	**show ip ospf** [*process-id*] **neighbor** [**detail**] [*interface-typeinterface-number*] [*neighbor-id*]
Displays the OSPF routing table.	**show ip ospf** [*process-id*] **route**[**count**]
Displays the number of times SPT is computed in the OSPF area.	**show ip ospf** [*process-id*] **spf**
Displays the summarized route of OSPF redistributed routes.	**show ip ospf**[*process-id*] **summary-address**
Displays OSPF virtual links.	**show ip ospf** [*process-id*] **virtual-links** [*ip-address*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs OSPF events.	**debug ip ospf events** [**abr**|**asbr**|**lsa**|**nssa**|**os**|**restart**| **router**|**slink**| **vlink**]
Debugs OSPF interfaces.	**debug ip ospf ifsm** [**events**|**status**|**timers**]
Debugs OSPF neighbors.	**debug ip ospf nfsm** [**events** | **status** | **timers**]
Debugs the OSPF NSM.	**debug ip ospf nsm** [**interface** | **redistribute** | **route**]
Debugs OSPF LSAs.	**debug ip ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Debugs OSPF packets.	**debug ip ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
Debugs OSPF routes.	**debug ip ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

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

3 Configuring RIPng

3.1 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 the autonomous system (AS) and is applicable to small-sized networks with routes no more than 16 hops.

Protocols and Standards

- RFC2080: Defines the RIPng.

Note:

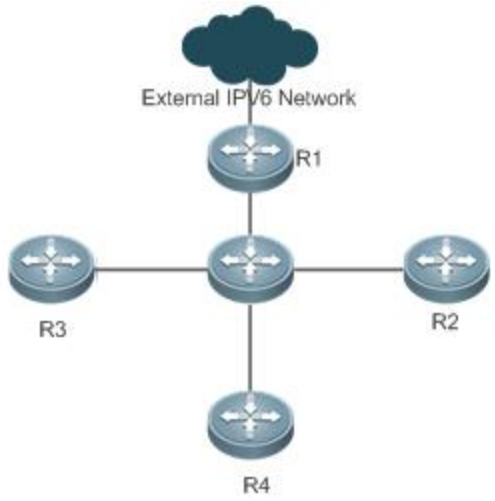
"Router" in this chapter refers to the network device that supports the routing function. These network devices can be Layer 3 switches, routers, firewalls, etc.

3.2 Application

RIPng is generally used on some small-sized networks, such as office networks of small companies.

As shown in the following figure, the company builds an IPv6 network, on which all routers support IPv6. The network is small in size, but the workload is still heavy if the network is maintained manually. In this case, RIPng can be configured to adapt to topological changes of the small-sized network, which reduces the workload.

Figure 4-1



3.3 Features

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.

Feature

Feature	Description
RIPng and RIP	RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations.
Exchanging Routing Information	By exchanging routing information, RIPng-enabled devices can automatically obtain routes to a remote network and update routes in real time.
Routing Algorithm	RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.
Avoiding Route Loops	RIPng uses functions, such as split horizon and poison reverse, to avoid route loops.

3.3.1 RIPng and RIP

RIP applies to IPv4 networks. Two RIP versions are available, including RIPv1 and RIPv2.

RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations.

Working Principle

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.

RIPng

RIPng packets are multicast. The multicast address is FF02::9, the source address is FE80::/10, and the UDP port ID is 521. RIPng can identify the subnet mask.

This chapter describes functions and configurations of RIPng. For details about RIPv2, see "Configuring RIP".

Related Configuration

Enabling the RIPng Process

By default, the RIPng process is disabled.

Run the **ipv6 router rip** command to enable the RIPng process.

You must enable the RIPng process on a device; otherwise, all functions related to RIPng cannot take effect.

Running RIPng on an Interface

By default, RIPng does not run on an interface.
Run the **ipv6 rip enable** command to run RIPng on an 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.

Prohibiting an Interface from Sending or Receiving Packets

By default, a RIPng-enabled interface is allowed to send and receive RIPng packets.
Run the **passive-interface** command to prohibit an interface from sending RIPng packets.

3.3.2 Exchanging Routing Information

Compared with static routing, the dynamic routing protocol has a significant advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

Working Principle

Initialization

After RIPng is enabled on a router, the router sends a request packet to its neighbor router, requesting for all routing information, that is, the routing table. After receiving the request message, the neighbor router 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 a series of updates, all 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 (update timer), that is, the entire routing table is sent to neighbor routers.

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.

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 router, or sent to a neighbor router.

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.

Related Configuration

RIPng Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.
Run the **timers basic** command to modify durations of RIPng timers.
Increasing the duration of the flush timer can reduce the route flapping. Decreasing the duration of the flush timer helps accelerate route convergence.
The durations of RIPng timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to modify the RIPng timers.

Default Route

Run the **ipv6 rip default-information** command to advertise the default route to neighbors on an interface.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIPng and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit the routing information sent by the device.
Run the **distribute-list in** command to set filtering rules to limit the routing information received by the device.

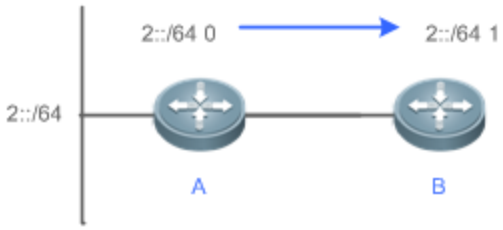
3.3.3 Routing Algorithm

RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

Working Principle

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 (metric). 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 (metric) 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 between 0 and 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 to a large-scale network.
As shown in the following figure, Router A is connected to the network 2::/64. Router B obtains the route (2::/64, 0) from Router A and adds the metric 1 to the route to obtain its own route (2::/64, 1), and the next hop points to Router A.
Figure 4-2

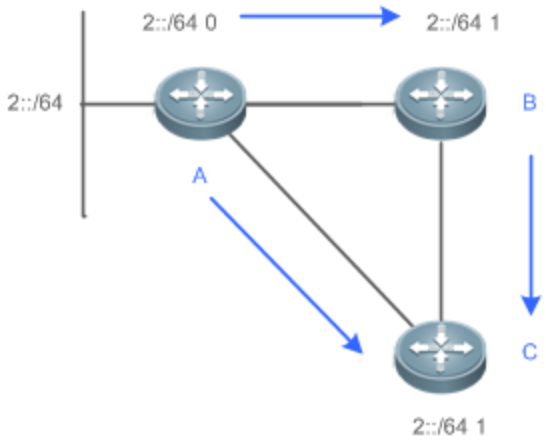


Selecting the Optimum Route

RIPng selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a router preferentially selects the route with the smallest metric.

As shown in the following figure, Router A is connected to the network 2::/64. Router C obtains the route (2::/64, 0) from Router A and the route (2::/64, 1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (2::/64, 1), and the next hop points to Router A.

Figure 4-3



When routes coming from different sources exist on a router, the route with the smaller distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
RIPng route	120
Unreachable route	255

Related Configuration

Modifying the Distance

By default, the distance of a RIPng route is 120.

Run the **distance** command to modify the distance of a RIPng route.

Modifying the Metric

For a RIPng route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. The metric offset of the interface is 1.
For a RIPng router that is manually configured (default route or redistributed route), the default metric is 1.
Run the **ipv6 rip metric-offset** command to modify the metric offset of the interface.
Run the **default-metric** command to modify the default metric of an external route (redistributed route).
Run the **redistribute** command to modify the metric of an external route (redistributed route) when advertising this route.
Run the **ipv6 rip default-information** command to modify the metric of a default route when advertising the default route.

3.3.4 Avoiding Route Loops

RIPng uses functions, such as split horizon and poison reverse, to avoid route loops.

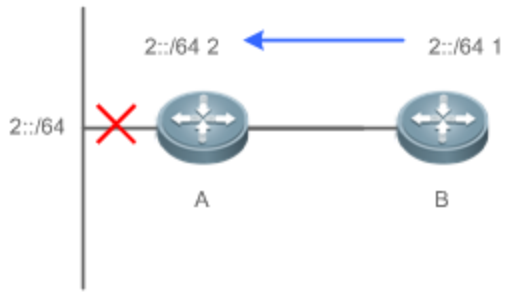
Working Principle

Route Loop

A RIPng route loop occurs due to inherent defects of the distance-vector algorithm.

As shown in the following figure, Router A is connected to the network 2::/64, and sends an update packet every 30s. Router B receives the route to 2::/64 from Router A every 30s. If Router A is disconnected from 2::/64, the route to 2::/64 will be deleted from the routing table on Router A. Next time, the update packet sent by Router A no longer contains this route. As Router B does not receive an update packet related to 2::/64, Router B determines that the route to 2::/64 is valid within 180s and uses the update packet to send this route to Router A. As the route to 2::/64 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 2::/64 through Router A, and Router A determines that data can reach 2::/64 through Router B. In this way, a route loop is formed.

Figure 4-4

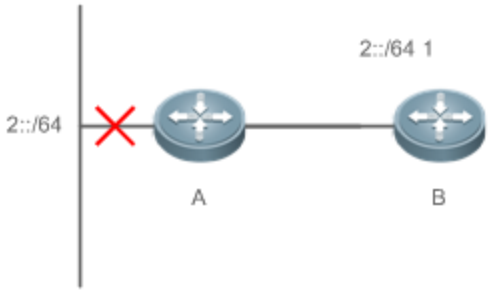


Split Horizon

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 the following figure, after split horizon is enabled on Router B, Router B will not send the route to 2::/64 back to Router A. Router B will learn 180s later that 2::/64 is not reachable.

Figure 4-5



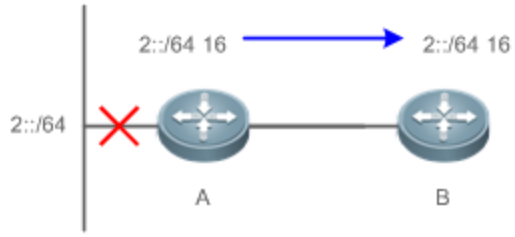
Poison Reverse

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 ag ain, but the metric of this router will be changed to 16 (unreachable).

As shown in the following figure, after poison reverse is enabled on Router A, if Route A detects a disconnection from 2::/64 , Router A will not delete the route to 2::/64. Instead, Router A changes the number of hops to 16, and advertises the route through the update packet. On receiving the update packet, Router B learns that 2::/64 is not reachable.

Figure 4-6



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **split-horizon poisoned-reverse** command to enable poison reverse. (After poison reverse is enabled, split horizon is automatically disabled.)

3.4 Configuration

Configuration	Related Commands	
Configuring RIPng Basic Functions	(Mandatory) It is used to build a RIPng routing domain.	
	ipv6 router rip	Enables a RIPng routing process and enters routing process configuration mode.
	ipv6 rip enable	Runs RIPng on an interface.
	split-horizon	Enables split horizon or poison reverse.
	passive-interface	Configures a passive interface.
Advertising the Default Route or External Routes	Optional.	
	ipv6 rip default-information	Advertise the default route to neighbors on an interface.
	redistribute	Redistributes routes and advertising external routes to neighbors.
Setting Route Filtering Rules	Optional.	
	distribute-list in	Filters the received RIPng routing information.
	distribute-list out	Filters the sent RIPng routing information.
Modifying Route Selection Parameters	Optional.	
	distance	Modifies the administrative distance of a RIPng route.
	ipv6 rip metric-offset	Modifies the metric offset on an interface.
	default-metric	Configure the default metric for route redistribution.
Modifying Timers	Optional.	
	timers	Modifies the update timer, invalid timer, and flush timer of RIPng.

3.4.1 Configuring RIPng Basic Functions

Configuration Effect

- Build a RIPng routing domain on the network.
- Routers in the domain obtain routes to a remote network through RIPng.

Notes

- IPv6 addresses must be configured.
- IPv6 unicast routes must be enabled.

Configuration Steps

↘ **Enabling a RIPng Routing Process**

- Mandatory.
- Unless otherwise required, perform this configuration on every router in the RIPng routing domain.

Running RIPng on an Interface

- Mandatory.
- Unless otherwise required, perform this configuration on every interconnected interface of routers in the RIPng routing domain.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on every interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on every interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected 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, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- This configuration is recommended.
- Use the passive interface to set the boundary of the 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.
- 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.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIPng.

Related Commands

Enabling a RIPng Routing Process

Command	**ipv6 router rip**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to create a RIPng routing process and enter routing process configuration mode.

Running RIPng on an Interface

Command	**ipv6 rip enable**

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The configuration for running the RIPng on an interface is different from that of RIPv2. In RIPv2, the **network** command is configured in routing process configuration mode to define an IP address range. If the IP address of an interface belongs to this IP address range, RIP automatically runs on this interface.

Enabling Split Horizon

Command	**split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates that the split horizon function contains the poison reverse function.
Command Mode	Routing process configuration mode
Usage Guide	Run the **show ipv6 rip** command to check whether split horizon is enabled. The configuration is different from that of RIPv2. In RIPv2, the split horizon function is configured in interface configuration mode.

Configuring a Passive Interface

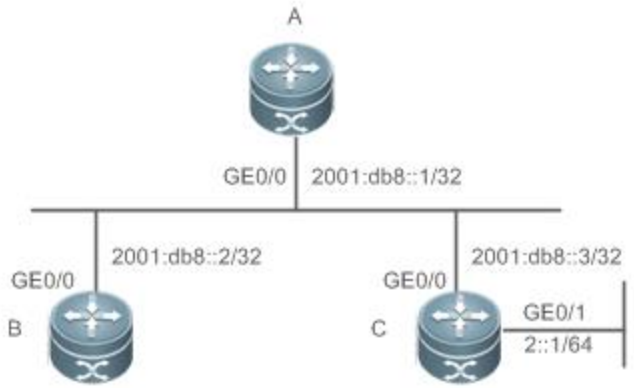
Command	**passive-interface** { **default** | *interface-type interface-num* }
Parameter Description	**default:** Indicates all interfaces. ***interface-type interface-num*:** Specifies an interface.
Command Mode	Routing process configuration mode
Usage Guide	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command so that the interfaces used for interconnection between routers in the domain are not passive interface.

Displaying the IP Routing Table

Command	**show ipv6 route**
Parameter Description	N/A
Command Mode	Privileged EXEC mode or global configuration mode
Usage Guide	Check whether the routing table contains any route to a remote network that is learned through RIPng.

Configuration Example

Building a RIPng Routing Domain

Scenario **Figure 4-7**	
Configuration Steps	● Configure IPv6 addresses on all routers. ● Enable RIPng on all routers.
A	A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# ipv6 router rip A(config-router)# exit A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32 A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
B	B# configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)# ipv6 router rip B(config-router)# exit B(config)# interface GigabitEthernet 0/0 B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32 B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
C	C# configure terminal Enter configuration commands, one per line. End with CNTL/Z. C(config)# ipv6 router rip C(config-router)# exit C(config)# interface GigabitEthernet 0/0 C(config-if-GigabitEthernet 0/0)#

	C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32 C(config-if-GigabitEthernet 0/0)# ipv6 rip enable C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64 C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
Verification	Check the routing tables on Router A, Router B, and Router C. The routing tables should contain routes to a remote network that are learned through RIPng.
A	A# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::1/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
B	B# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

```
        IA - Inter area


R       2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0
C       2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L       2001:DB8::2/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
```

C

```
Hostname# show ipv6 route


IPv6 routing table name - Default - 9 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area


C       2::/64 via GigabitEthernet 0/1, directly connected
L       2::2/128 via GigabitEthernet 0/1, local host
C       2001:DB8::/32 via GigabitEthernet 0/0, directly connected
L       2001:DB8::3/128 via GigabitEthernet 0/0, local host
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host
```

This series does not support ISIS or BGP. The configuration example is only for reference.

Common Errors

- The IPv6 address is not configured on an interface.
- The interface used for interconnection between devices is configured as a passive interface.

3.4.2 Advertising the Default Route or External Routes

Configuration Effect

- In the RIPng domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIPng domain.
- In the RIPng domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIPng domain.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

↘ Configuring External Route Redistribution

- Optional.
- Perform this configuration if external routes of the RIPng domain should be introduced to the AS border router (ASBR).

↘ Generating a Default Route

- Optional.
- Perform this configuration if the default route should be introduced to an ASBR so that other routers in the RIPng domain access other AS domains through this ASBR by default.

Verification

- Run the **show ipv6 route rip** command on a non-ASBR to check whether the external routes of the domain and default route have been loaded.

Related Commands

↘ Advertising the Default Route to Neighbors on an Interface

Command	**ipv6 rip default-information** { **only**|**originate** } [**metric** *metric-value*]
Parameter Description	**only**: Advertises only IPv6 default route. **originate**: Advertises the IPv6 default route and other routes. **metric** *metric-value*: Indicates the metric of the default route. The value ranges from 1 to 15. The default value is 1.
Command Mode	Interface configuration mode
Usage Guide	After 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 or 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.

Redistributing Routes and Advertising External Routes to Neighbors

Command	**redistribute** { **connected** | **static** } [**metric** *metric-value* | **route-map** *route-map-name*]
Parameter Description	**connected**: Indicates redistribution from direct routes. **static**: Indicates redistribution from static routes. **metric** *metric-value*: Sets the metric of the route redistributed to the RIPng domain. **route-map** *route-map-name*: Sets the redistribution filtering rules.
Command Mode	Routing process configuration mode
Usage Guide	During route redistribution, it is not necessary to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use completely different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other.

Configuration Example

Scenario **Figure 4-8**	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router B, configure redistribution of static routes. ● On the GE0/1 interface of Router A, configure advertisement of the default route.

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information originate`

B	`B# configure terminal`
	`B(config)# ipv6 router rip`
	`B(config-router)# redistribute static`

Verification	● Check the routing tables on Router A and Router B, and confirm that Router A can learn the route 3001:10:10::/64, and Router B can learn the default route ::/0.

A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
B	B# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1

This series does not support ISIS or BGP. The configuration example is only for reference.

3.4.3 Setting Route Filtering Rules

Configuration Effect

- 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.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

↘ **Filtering the Received RIP Routing Information**

- To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.

Filtering the Sent RIP Routing Information

- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.

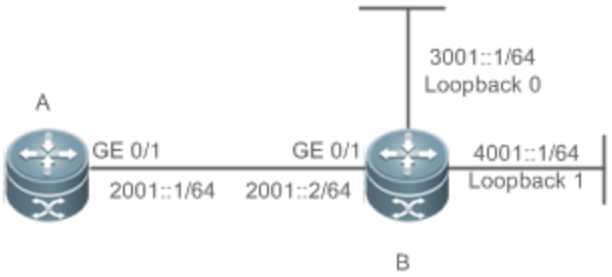
Verification

- Run the **show ipv6 route rip** command to check that the routes that have been filtered out are not loaded to the routing table.

Related Commands

Command	**distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]
Parameter Description	**prefix-list** *prefix-list-name:* Indicates the name of the prefix list, which is used to filter routes. **in** | **out:** Specifies update routes (received or sent routes) that are filtered. *interface-type interface-name:* Indicates that the distribution list is applied to the specified interface.
Command Mode	Routing process configuration mode
Usage Guide	N/A

Configuration Example

Scenario Figure 4-9	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On router A, configure route filtering.

A	`A# configure terminal`
	`A(config)# ipv6 prefix-list hello permit 4001::/64`
	`A(config)# ipv6 router rip`
	`A(config-router)# distribute-list prefix-list hello in`

Verification	● Check that Router A can learn only the route to 4001::/64.

A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 4001::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

This series does not support ISIS or BGP. The configuration example is only for reference.

3.4.4 Modifying Route Selection Parameters

Configuration Effect

- 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.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

Modifying the Administrative Distance of a RIPng Route

- Optional.
- Perform this configuration if you wish to change the priorities of RIPng routes on a router that runs multiple unicast routing protocols.

Modifying the Metric Offset on an Interface

- Optional.
- Unless otherwise required, perform this configuration on a router where the metrics of routes need to be adjusted.

Configuring the Default Metric of an External Route Redistributed to RIPng

- Optional.
- Unless otherwise required, perform this configuration on an ASBR to which external routes are introduced.

Verification

- Run the **show ipv6 rip** command to display the administrative distance of RIPng routes.

- Run the **show ipv6 rip data** command to display the metrics of external routes redistributed to RIPng.

Related Commands

Modifying the Administrative Distance of a RIPng Route

Command	**distance** *distance*
Parameter Description	*distance*: Sets the administrative distance of a RIPng route. The value is an integer ranging from 1 to 254.
Command Mode	Routing process configuration mode
Usage Guide	Run this command to set the administrative distance of a RIPng route.

Modifying the Metric Offset on an Interface

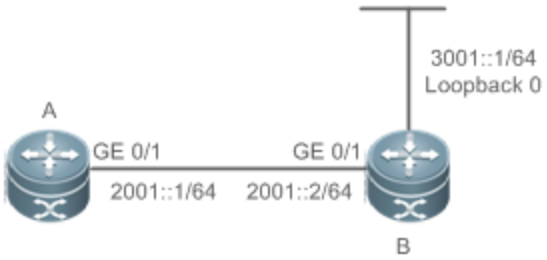
Command	**ipv6 rip metric-offset** *value*
Parameter Description	*value*: Indicates the interface metric offset. The value ranges from 1 to 16.
Command Mode	Routing process configuration mode
Usage Guide	Before a route is added to the routing table, the metric of the route must be added with the metric offset set on the interface. You can control the use of a route by setting the interface metric offset.

Configuring the Default Metric of an External Route Redistributed to RIPng

Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric. The valid value ranges from 1 to 16. If the value is equal to or greater than 16, the system determines that this route is unreachable.
Command Mode	Global configuration mode
Usage Guide	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. If this command is not configured, the value of **default-metric** is 1.

Configuration Example

Modifying the Administrative Distance of a RIPng Route

Scenario **Figure 4-10**	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router A, set the administrative distance of a RIPng route to 160.
	A# configure terminal A(config)# ipv6 router rip A(config-router)# distance 160
Verification	● On Router A, check whether the administrative distance of a RIPng route is 160.
	A# show ipv6 route rip | in 3001::/64 R 3001::/64 [160/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

3.4.5 Modifying Timers

Configuration Effect

- Change the duration of RIPng timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- 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.

Configuration Steps

↘ **Modifying the Update Timer, Invalid Timer, and Flush Timer**

- Mandatory.
- Unless otherwise required, perform this configuration on a router where RIPng timers need to be modified.

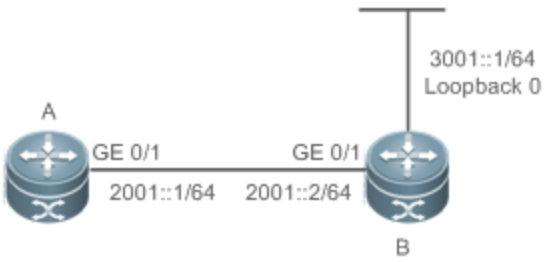
Verification

- Run the **show ipv6 rip** command to display settings of timers.

Related Commands

Command	**timers** *update invalid flush*
Parameter Description	*Update:* Indicates the route update time in second. It defines the interval at which the device sends the route update packet. Each time an update packet is received, the invalid timer and flush timer are reset. By default, a route update packet is sent every 30s. *Invalid:* Indicates the route invalid time in second, counted from the last time when a valid update packet is received. It defines the time after which the route in the routing list becomes invalid because the route is not updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the update packet is received before the invalid timer expires, the timer is reset. The default duration of the invalid timer is 180s. *Flush:* Indicates the route flushing time in second, counted from the time when the RIPng route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Usage Guide	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Configuration Example

Scenario **Figure 4-11**	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router A, configure the update timer, invalid timer, and flush timer.

B	`B# configure terminal`
	`B(config)# ipv6 router rip`
	`B(config-router)# timers 10 30 90`

Verification	● On Router B, check the settings of RIPng timers.

B	B# show ipv6 rip Routing Protocol is "RIPng" Sending updates every 10 seconds with +/-50%, next due in 12 seconds Timeout after 30 seconds, garbage collect after 90 seconds Outgoing update filter list for all interface is: not set Incoming update filter list for all interface is: not set Default redistribution metric is 1 Default distance is 120 Redistribution: Redistributing protocol connected Default version control: send version 1, receive version 1 Interface Send Recv GigabitEthernet 0/1 1 1 Routing Information Sources: Gateway: fe80::2d0:f8ff:fe22:334a Distance: 120 Last Update: 00:00:02 Bad Packets: 0 Bad Routes: 0

Common Errors

- Settings of RIPng timers on devices connected to the same network are inconsistent. Consequently, routes cannot be learned properly.

3.5 Monitoring

Displaying

Description	Command
Displays information about the RIPng process.	**show ipv6 rip**
Displays the RIPng routing table.	**show ipv6 rip database**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs RIPng.	**debug ipv6 rip** [interface *interface-type interface-num* | nsm | restart

4 Managing Routes

4.1 Overview

The network service module (NSM) 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. These routes are generally classified by source into three types:

- 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.

4.2 Applications

Application	Description
Basic Functions of the Static Route	Manually configure a route.
Floating Static Route	Configure a standby route in the multipath scenario.
Load Balancing Static Route	Configure load balancing static routes in the multipath scenario.

4.2.1 Basic Functions of the Static Route

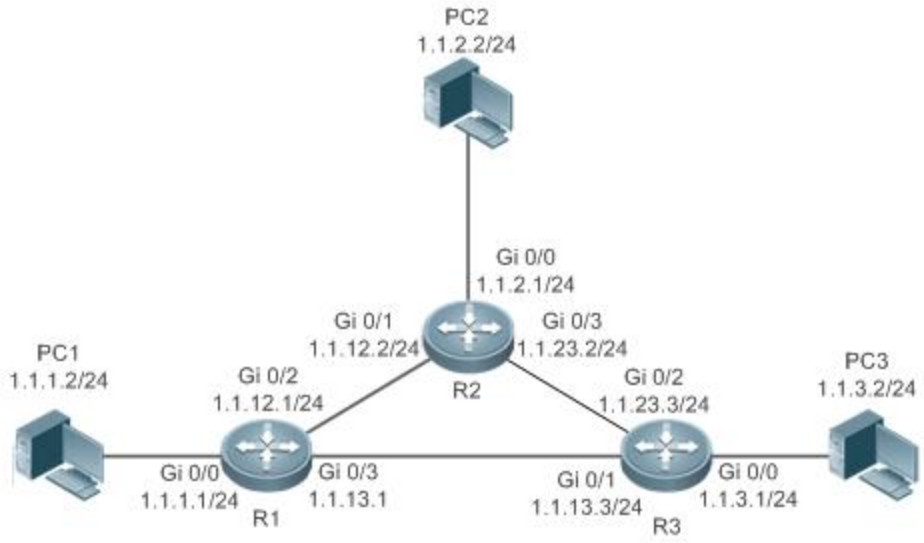
Scenario

On a network with a simple topology, you can configure only static routes to implement network interworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

As shown in Figure 5-1, to implement interworking between PC 1, PC 2, and PC 3, you can configure static routes on R 1, R 2, and R 3.

- On R 1, configure a route to the network segment of PC 2 through R 2, and a route to the network segment of PC 3 through R 3.
- On R 2, configure a route to the network segment of PC 1 through R 1, and a route to the network segment of PC 3 through R 3.
- On R 3, configure a route to the network segment of PC 1 through R 1, and a route to the network segment of PC 2 through R 2.

Figure 5-1



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, and R 3.

4.2.2 Floating Static Route

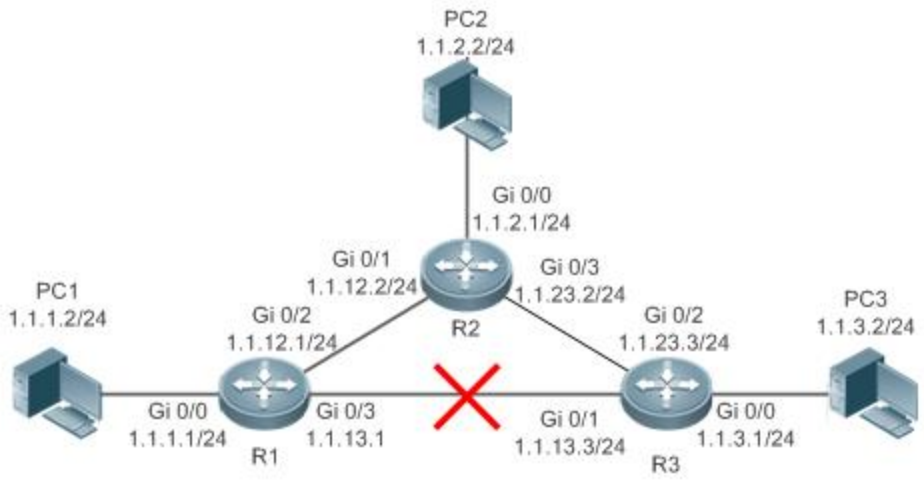
Scenario

If no dynamic routing protocol is configured, you can configure floating static routes to implement dynamic switching of routes to prevent communication interruption caused by the network connection failures.

As shown in Figure 5-2, to prevent communication interruption caused by a line failure between R 1 and R 3, you can configure a floating static route respectively on R 1 and R 3. Normally, packets are forwarded on a path with a small administrative distance. If a link on this path is down, the route is automatically switched to the path with a large administrative distance.

- On R1, configure two routes to the network segment of PC 3, including a route through R 3 (default distance = 1) and a route through R 2 (default distance = 2).
- On R 3, configure two routes to the network segment of PC 1, including a route through R 1 (default distance = 1) and a route through R 2 (default distance = 2).

Figure 5-2



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, and R 3.

4.2.3 Load Balancing Static Route

Scenario

If there are multiple paths to the same destination, you can configure load balancing routes. Unlike floating route s, the administrative distances of load balancingroutes are the same. Packets are distributed among these routes based on the balanced forwarding policy.

As shown in Figure 5-3, load balancing routes are configured respectively on R 1 and R 3 so that packets sent to the network segment of PC 3 or PC 1 are balanced between two routes, including a route through R 2 and a route through R 4.

- On R 1, configure two routes to the network segment of PC 3, including a route through R 2 and a route through R 4.
- On R 3, configure two routes to the network segment of PC 1, including a route through R 2 and a route through R 4.

Figure 5-3



Remarks	On the switch, the load is balanced based on the source IP address by default. Run the **aggregateport load-balance** command to configure the load balancing mode of ECMP route.

Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, R 3, and R 4.
- Configure the load balancing policy on R 1 and R 3.

4.3 Features

Feature	Description
Route Computation	Generate a valid route on a device.
Optimal Route Selection	Select an optimal route to forward packets.
Default Route	Forward all packets and help reduce the size of a routing table.
Route Reliability	Quickly detect a route failure and recover communication.

4.3.1 Route Computation

Routing Function

Routing functions are classified into IPv4 and IPv6 routing functions. If the routing functions are disabled, a device is equivalent to a host and cannot forward routes.

Dynamic Route

A dynamic routing protocol learns remote routes and dynamically updates routes by exchanging routes with neighbors. If a neighbor is the next hop of a route and this neighbor fails, the route fails as well.

Static Route

On a network with a simple topology, you can configure only static routes to implement network interworking. 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 (L3) 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.

4.3.2 Optimal Route Selection

Administrative Distance

When multiple routing protocols generate routes to the same destination, the priorities of these routes can be determined based on the administrative distance. A smaller administrative distance indicates a higher priority.

Equal-Cost Route

If multiple routes to the same destination have different next hops but the same administrative 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.

Floating Route

If multiple routes to the same destination have different next hops and different administrative distances, these routes are mutually floating routes. The route with the smallest administrative distance will be first selected for packet forwarding. If this route fails, a route with a larger administrative distance is further selected for forwarding, thus preventing communication interruption caused by a network line failure.

4.3.3 Default Route

In the 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 L2 switch, the **ip default gateway** command is configured to generate a default route.

Static Default Route

On a L3 switch, a static route with the network segment 0.0.0.0 and the subnet mask 0.0.0.0 is configured to generate the 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.

4.3.4 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.

4.4 Configuration

Configuration Item	Description and Command	
Configuring a Static Route	(Mandatory) It is used to configure a static route entry.	
	ip route	Configures an IPv4 static route.
	ipv6 route	Configures an IPv6 static route.
Configuring a Default Route	(Optional) It is used to configure the default gateway.	
	ip default gateway	Configures an IPv4 default gateway on a L2 device.
	ipv6 default gateway	Configures an IPv6 default gateway on a L2 device.
	ip route 0.0.0.0 0.0.0.0 *gateway*	Configures an IPv4 default gateway on a L3 device.
	ipv6 route ::/0 *ipv6-gateway*	Configures an IPv6 default gateway on a L3 device.
	ip default network	Configures an IPv4 default network on a L3 device.
Configuring Route Limitations	(Optional) It is used to limit the number of equal-cost routes and number of static routes, or disable routing.	
	maximum-paths	Configures the maximum number of equal-cost routes.
	ip static route-limit	Configures the maximum number of IPv4 static routes.
	ipv6 static route-limit	Configures the maximum number of IPv6 static routes.

Configuration Item	Description and Command	
	no ip routing	Disables IPv4 routing.
	noipv6 unicast-routing	Disables IPv6 routing.

4.4.1 Configuring a Static Route

Configuration Effect

- Generate a static route in the routing table. Use the static route to forward packets to a remote network.

Notes

- Static routes cannot be configured on a L2 switch.
- If the **no ip routing** command is configured on a L3 switch, 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 L3 switch, 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.

Configuration Steps

↘ Configuring a Static IPv4 Route

Configure the following command on an IPv4-enabled routing device.

Command	**ip route** *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent** [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**]	
Parameter Description	*network*	Indicates the address of the destination network.
	net-mask	Indicates the mask of the destination network.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface*, or both of them. If *ip-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface*, or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.

	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	disabled/enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route** *network net-mask ip-address.*	

Configuring an IPv6 Static Route

Configure the following command on an IPv6-enabled router.

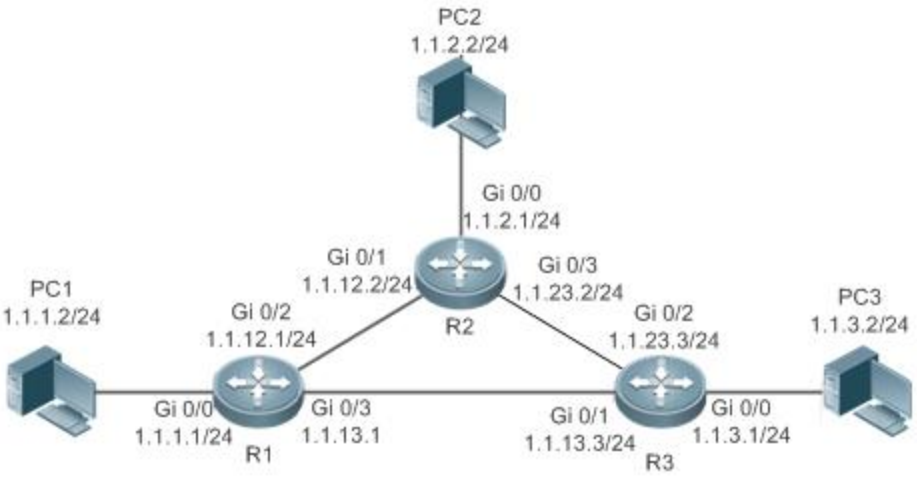
Command	**ipv6 route** *ipv6-prefix/prefix-length* { *ipv6-address* [*interface* [*ipv6-address* [*distance*] [**weight***number*] [**description***description-text*]	
Parameter Description	*ipv6-prefix*	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	prefix-length	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route***ipv6-prefix / prefix-length ipv6-address.*	

Verification

- Run the **show ip route** command to display the IPv4 routing table and check whether the configured IPv4 static route takes effect.
- Run the **show ipv6 route** command to display the IPv6 routing table and check whether the configured IPv6 static route takes effect.

Configuration Example

Configuring Static Routes to Implement Interworking of the IPv4 Network

Scenario **Figure 5-4**	
Configuration Steps	• Configure interface addresses on each device.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit

	R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/3 R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
R3	R3#configure terminal R3(config)#interface gigabitEthernet 0/0 R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/1 R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/2 R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
	● Configure static routes on each device.
R1	R1#configure terminal R1(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2 R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
R2	R2#configure terminal R2(config)#ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1 R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
R3	R3#configure terminal R3(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2 R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
Verification	● Displaythe routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2

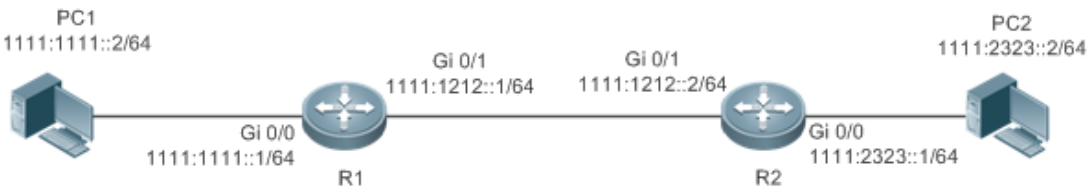
	SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. S 1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2 S 1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host.
R2	R2# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0 C 1.1.2.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.2.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.2/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.23.2/32 is local host.
R3	R3# show ip route Codes: C - Connected, L - Local, S - Static

```
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
S      1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2
S      1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2
C      1.1.3.0/24 is directly connected, GigabitEthernet 0/0
C      1.1.3.1/32 is local host.
C      1.1.13.0/24 is directly connected, GigabitEthernet 0/1
C      1.1.13.3/32 is local host.
C      1.1.23.0/24 is directly connected, GigabitEthernet 0/2
C      1.1.23.3/32 is local host.
```

This series does not support ISIS or BGP. The configuration example is only for reference.

Configuring Static Routes to Implement Interworking of the IPv6 Network

Scenario **Figure 5-5**	
Configuration Steps	● Configure interface addresses on each device.

R1	`R1#configure terminal`
	`R1(config)#interface gigabitEthernet 0/0`
	`R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64`
	`R1(config-if-GigabitEthernet 0/0)# exit`
	`R1(config)#interface gigabitEthernet 0/1`
	`R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64`

R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64
	● Configure static routes on each device.
R1	R1#configure terminal R1(config)# ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
R2	R2#configure terminal R2(config)#ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
Verification	● Displaythe routing table.
R1	R1# show ipv6 route IPv6 routing table name - Default - 10 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 C 1111:1111::/64 via GigabitEthernet 0/0, directly connected L 1111:1111::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host

	C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
R2	R2# show ipv6 route IPv6 routing table name - Default - 10 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 C 1111:2323::/64 via GigabitEthernet 0/0, directly connected L 1111:2323::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host

This series does not support ISIS or BGP. The configuration example is only for reference.

Common Errors

- The link on the interface is not up.
- No IP address is configured for the interface.

4.4.2 Configuring a Default Route

Configuration Effect

- Generate a default route in the routing table. The default route is used to forward packets that cannot be forwarded by other routes.

Notes

- On a L2 switch, run the **ip default gateway** or **ipv6 default gateway** command to configure the default gateway.
- On a L3 switch, run the **ip route** 0.0.0.0 0.0.0.0 *gateway* or **ipv6 route** ::/0 *ipv6-gateway* command to configure the default gateway.
- If the **no ip routing** or **no ipv6 unicast- routing** command is configured on a L3 switch, you can run the **ip default gateway** or **ipv6 default gateway** command to configure the default gateway.

Configuration Steps

Configuring the IPv4 Gateway on a L2 Switch

Command	**ip default-gateway** *gateway*	
Parameter Description	*gateway*	indicates the IPv4 gateway address.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuring the IPv6 Gateway on a L2 Switch

Command	**ipv6 default-gateway** *gateway*	
Parameter Description	*gateway*	indicates the IPv6 gateway address.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuring the IPv4 Default Gateway on a L3 Switch

Command	**ip route 0.0.0.00.0.0.0**{ *ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**]	
Parameter Description	**0.0.0.0**	Indicates the address of the destination network.
	0.0.0.0	Indicates the mask of the destination network.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *interface* is not specified, a

		recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	disabled /enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route0.0.0.0 0.0.0.0** *ip-address.*	

Configuring the IPv6 Default Gateway on a L3 Switch

Command	**ipv6 route::/0** { *ipv6-address* | *interface* [*ipv6-address* } [*distance*] [**weight***number*] [**description***description-text*]	
Parameter Description	**::**	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	0	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	Ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static default route is configured.	

Command Mode	Global configuration mode
Usage Guide	The simplest configuration of this command is **ipv6 route** ::/0 *ipv6-gateway*.

Configuring the IPv4 Default Network on a L3 Switch

Command	**ip default-network** *network*	
Parameter Description	*network*	Indicates the address of the network. (The network must be a Class A, B, or C network.)
Defaults	By default, no default network is configured.	
Command Mode	Global configuration mode	
Usage Guide	If the network specified by the **ip default-network** command exists, 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.	

Verification

- On a L2 switch (or a L3 switch where routing is disabled), run the **show ip redirects** or **show ipv6 redirects** command to display the default gateway.
- On a L3 switch where routing is enabled, run the **show ip route** or **show ipv6 route** command to display the default route.

Configuration Example

Configuring IPv4 Default Routes on L3 Switches to Implement Network Interworking

Scenario Figure 5-6	
Configuration Steps	● Configure IP addresses on L3 devices.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0

	R1(config-if-GigabitEthernet 0/0)# exit
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit
R1	● Configure an IPv6 default gateway on R 1. R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.2
R2	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.1
Verification	● Displaythe routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is 1.1.12.2 S* 0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1 C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.1/32 is local host. This series does not support ISIS or BGP. The configuration example is only for reference.

4.4.3 Configuring Route Limitations

Configuration Effect

- Limit the number of equal-cost routes and number of static routes, or disable routing.

Notes

Route limitations cannot be configured on a L2 switch.

Configuration Steps

Configuring the Maximum Number of Equal-Cost Routes

Command	**maximum-paths** *number*	
Parameter Description	*number*	Indicates the maximum number of equal-cost routes. The value is 1.
Defaults	The default value varies with the device model.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of next hops in the equal-cost route. In load balancing mode, the number of routes on which traffic is balanced does not exceed the configured number of equal-cost routes.	

Configuring the Maximum Number of IPv4 Static Routes

Command	**ip static route-limit** *number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1, 024 IP static routes can be configured.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of IPv4 static routes. If the maximum number of IPv4 static routes is reached, no more IPv4 static route can be configured.	

Configuring the Maximum Number of IPv6 Static Routes

Command	**ipv6 static route-limit** *number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1,000 IPv6 static routes can be configured.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of IPv6 static routes. If the maximum number of IPv6 static routes is reached, no more IPv6 static route can be configured.	

Disabling IPv4 Routing

Command	**no ip routing**
Parameter Description	N/A
Defaults	By default, IPv4 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv4 routing. If the device functions only as a bridge or a voice over IP (VoIP) gateway, the device does not need to use the IPv4 routing function of the system. In this case, you can disable the IPv4 routing function of the system.

Disabling IPv6 Routing

Command	**no ipv6 unicast-routing**
Parameter Description	N/A
Defaults	By default, IPv6 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 routing. If the device functions only as a bridge or a VoIP gateway, the device does not need to use the IPv6 routing function of the system. In this case, you can disable the IPv6 routing function of the system.

4.5 Monitoring

Displaying

Description	Command
Displays the IPv4 routing table.	**show ip route**
Displays the IPv6 routing table.	**show ipv6route**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs IPv4 route management.	**debug nsm kernel ucast- v4**
Debugs IPv6 route management.	**debug nsm kernel ucast-v6**
Debugs default network management.	**debug nsm kernel default-network**
Debugs internal events of route	**debug nsm events**

management.	
Debugs sending of route management and routing protocol messages.	**debug nsm packet send**
Debugs receiving of route management and routing protocol messages.	**debug nsm packet recv**

Multicast Configuration

1. Configuring IP Multicasting
2. Configuring IGMP Snooping

1 Configuring IP Multicasting

1.1 Overview

IP multicasting is abstracted hardware multicasting and an extended multicast routing protocol on the standard IP network layer.

In traditional IP transmission, only one host can send packets to a single host (unicast communication) or all hosts (broadcast communication). However, the multicast technology provides the third choice: a host can send packets to certain specified hosts.

IP multicasting is applicable to one-to-many multimedia applications.

1.2 Features

Overview

Feature	Description
Configuring Layer-2 Direction Control for Multicast Streams	Allows a specified multicast stream to be configured with multiple commands, that is, to be configured with multiple ports that can forward the stream. Once direction control is configured for a multicast stream, the stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream.
Configuring Multicast Non-Stop Forwarding Parameters	During normal running, SSP synchronizes the hardware multicast forwarding table to the management board in real time. After the management board is switched, the command for configuring the multicast control plane of the original slave management board is loaded, and the multicast protocol (such as PIM-SM or IGMP Snooping) re-converges. The multicast non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of the multicast protocol.
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	Deletes the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

1.2.1 Configuring Layer-2 Direction Control for Multicast Streams

Configure layer-2 direction control for multicast streams to control the forwarding of multicast streams on an interface.

Working Principle

Configure layer-2 direction control for multicast streams and a forwarding interface so that multicast streams can be forwarded only through configured interfaces. In this case, layer-2 forwarding of multicast streams can be controlled.

Related Configuration

↘ Configuring Layer-2 Direction Control for Multicast Streams

By default, layer-2 direction control for multicast streams is disabled.

Run **ip multicast static** *source-address group-address interface-type interface-number* to configure layer-2 direction control for multicast streams.

1.2.2 Configuring Multicast Non-Stop Forwarding Parameters

The non-stop forwarding function ensures continuous forwarding of multicast data streams during the re-convergence of multicast protocols.

Working Principle

During normal running, SSP synchronizes the hardware multicast forwarding table to the management board in real time. After the management board is switched, the command for configuring the multicast control plane of the original slave management board is loaded, and the multicast protocol (such as PIM-SM or IGMP Snooping) re-converges. The multicast non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of multicast protocols.

After the configured protocol convergence period times out, all multicast forwarding table entries that are not updated during the convergence period are deleted.

Related Configuration

↘ Configuring the Maximum Period for Multicast Protocol Convergence

By default, the maximum period for multicast protocol convergence is 20s.

Run **msf nsf convergence-time** *time* to configure the maximum period for multicast protocol convergence. The value ranges from 0 to 3600s.

A larger value of *time* means a longer maximum period for multicast protocol convergence.

↘ Configuring the Multicast Packet Leakage Period

By default, the multicast packet leakage period is 30s.

Run **msf nsf leak** *interval* to configure the multicast packet leakage period. The value ranges from 0 to 3600s.

A larger value of interval means a longer leakage period.

1.2.3 Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Working Principle

Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Related Configuration

↘ **Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries**

By default, the overwriting mechanism upon the overflow of multicast hardware forwarding entries is disabled.

Run **msf ipmc-overflow override** to configure the overwriting mechanism upon overflow of multicast hardware forwarding entries.

1.3 Configuration

Configuration	Description and Command	
Configuring Layer-2 Direction Control for Multicast Streams	**ip multicast static** *source-address group-address interface-type interface-number*	Controls the direction of data streams on layer-2 interfaces.
Configuring Multicast Non-Stop Forwarding Parameters	**msf nsf convergence-time** *time*	Configures the maximum period for multicast protocol convergence.
	msf nsf leak *time*	Configures the multicast packet leakage period.
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	**msf ipmc-overflow override**	Configures the overwriting mechanism upon overflow of multicast hardware forwarding entries.

1.3.1 Configuring Layer-2 Direction Control for Multicast Streams

Configuration Effect

Configure layer-2 direction control for multicast streams to control the forwarding of multicast streams on an interface.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Layer-2 direction control for multicast streams can be configured on layer-2 devices unless otherwise specified.

Verification

Send multicast packets on the network containing layer-2 device A, connect multiple user hosts to VLAN 1 of layer-2 device A to receive the group, configure layer-2 direction control for multicast streams on device A, and check whether multicast packets are sent to the configured layer-2 interface.

Related Commands

Configuring Layer-2 Direction Control for Multicast Streams

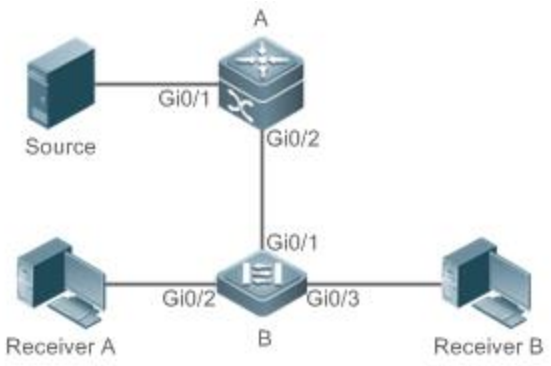
Command	**ip multicast static** *source-address group-address interface-type interface-number*
Parameter Description	*source -address*: Specifies the multicast source address. *group-address*: Specifies the multicast group address. *interface-type interface-number*: Specifies a layer-2 interface that is allowed to forward the multicast flow.
Command Mode	Global configuration mode
Usage Guide	Allow a specified multicast flow to be configured with multiple commands, that is, to be configured with multiple interfaces. Once direction control is configured for a multicast stream, the stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream. This command controls only the forwarding of multicast streams on the interface, but does not directly affect the processing of multicast protocols on the protocol packets. However, since certain features of the multicast protocol are driven by multicast data streams, behaviors of the multicast routing protocols may also be affected.

Configuration Example

Creating the IP Multicast Service on the IPv4 Network and Configuring Layer-2 Direction Control for Multicast Streams

Scenario

Figure 1-8



Configuration Steps

- Configure the basic functions of IP multicasting. (Omitted)
- Configure layer-2 direction control for multicast streams on device B so that the streams are sent only

	to the Gi 0/2 interface.
B	A# configure terminal A(config)# ip multicast static 192.168.1.100 233.3.3.3 gigabitEthernet0/2
Verification	Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.1). Enable receivers A and B to join G. ● Check multicast packets received by receiver A. Receiver B should not be able to receive multicast packets from G.

Common Errors

- An IPv4 unicast route is incorrectly configured.

1.3.2 Configuring Multicast Non-Stop Forwarding Parameters

Configuration Effect

- The non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of multicast protocols.

Notes

- The basic functions of IP multicast must be configured.

Configuration Steps

↘ Configuring the Maximum Period for Multicast Protocol Convergence

- The maximum period for multicast protocol convergence can be specified on each device unless otherwise specified.

↘ Configuring the Multicast Packet Leakage Period

- The multicast leakage period can be configured on each device unless otherwise specified.

Verification

Run **show msf nsf** to check the configured multicast non-stop forwarding parameters.

Related Commands

↘ Configuring the Maximum Period for Multicast Protocol Convergence

Command	**msf nsf convergence-time** *time*
Parameter Description	**convergence-time** *time*: Specifies the maximum period for multicast protocol convergence. The value ranges from 0 to 3600s. The default value is 20s.
Command Mode	Global configuration mode
Usage Guide	-

Configuring the Multicast Packet Leakage Period

Command	**msf nsf leak** *interval*
Parameter Description	**leak** *intervald*: Specifies the multicast packet leakage period. The value ranges from 0 to 3600s. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	-

Displaying Multicast Non-Stop Forwarding Configurations

Command	**show msf nsf**
Parameter Description	**-**
Command Mode	Privilege, global and interface configuration modes
Usage Guide	-

Configuration ExampleCreating the IP Multicast Service on the IPv4 Network and Configuring Convergence Time

Scenario Basic environment of the IP multicast service

Configuration Steps

- Configure the basic functions of IP multicast.
- Configure the maximum period for multicast protocol convergence.
- Configure the multicast packet leakage period.

A

```
A# configure terminal
A(config)# msf nsf convergence-time 200
A(config)# msf nsf leak 300
```

Verification Run **show msf nsf** to display multicast non-stop forwarding configurations.

A

```
A# show msf nsf
Multicast HA Parameters
------------------------------------------------+------+
protocol convergence timeout                    200 secs
flow leak interval                              300 secs
```

Common Errors

1.3.3 Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Configuration Effect

- Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- The overwriting mechanism upon overflow of multicast hardware forwarding entries can be configured on each device unless otherwise specified.

Verification

Run **show running-config** to check whether the overwriting mechanism upon overflow of multicast hardware forwarding entries is configured.

Related Commands

↘ Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Command	**msf ipmc-overflow override**
Parameter Description	**-**
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

↘ Creating the IP Multicast Service on the IPv4 Network and Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Scenario	Basic environment of the IP multicasting service (Omitted)
Configuration Steps	● Configure the basic functions of IP multicasting. (Omitted) ● Configure the overwriting mechanism upon overflow of multicast hardware forwarding entries.
A	A# configure terminal A(config)#msf ipmc-overflow override
Verification	Run **show running-config** to check whether the overwriting mechanism upon overflow of multicast hardware forwarding entries is configured.
A	A# show running-config ...

	msf ipmc-overflow override ...

1.3.4 Configuring Immediate Delivery of Multicast Entries to the Forwarding Plane

Configuration Effect

- A forwarding table generated based on a routing table contains entries guiding multicast packet forwarding. After configuring immediate delivery of multicast entries to the forwarding plane, the forwarding rules specified by the entries take effect immediately.

Notes

- N/A

Configuration Steps

- You configure the function of immediate delivery of multicast entries to the forwarding plane on each device if there is no special requirement.

Verification

Run **show running-config** to check whether the function of immediate delivery of multicast entries to the forwarding plane is configured.

Related Commands

↘ **Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries**

Command	**msf immediately-install**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

1.4 Monitoring

Clearing

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

Displaying

Description	Command
Displays the IPv4 multi-layer multicast forwarding table.	**show msf msc**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the processing of IPv4 multi-layer multicast packet forwarding.	**debug msf forwarding**
Debugs the operation on multi-layer multicast forwarding entries on an IPv4 network.	**debug msf msc**
Debugs the bottom-layer hardware processing of IPv4 multi-layer multicast packet forwarding.	**debug msf ssp**
Debugs the invocation of API interfaces provided by IPv4 multi-layer multicast forwarding.	**debug msf api**
Debugs the processing of multi-layer multicast forwarding events on an IPv4 network.	**debug msf event**

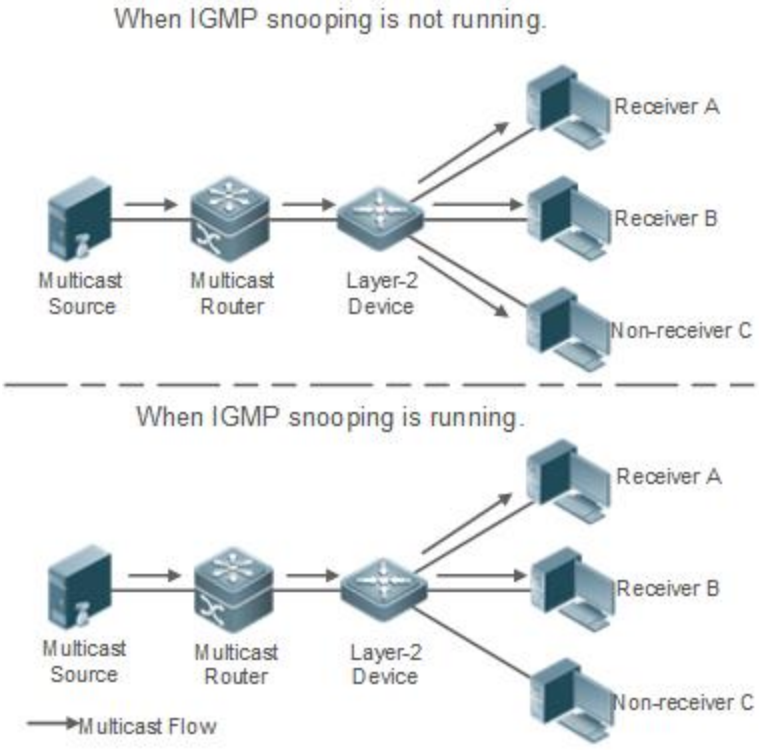
2 Configuring IGMP Snooping

2.1 Overview

Internet Group Management Protocol (IGMP) snooping is a mechanism of listening to IP multicast. It is used to manage and control the forwarding of IP multicast traffic within VLANs, realizing Layer-2 multicasting.

As shown in the following figure, when a Layer-2 device is not running IGMP snooping, IP multicast packets are broadcasted within the VLAN; when the Layer-2 device is running IGMP snooping, IP multicast packets are transmitted only to profile members.

Figure 2-1 Networking Topology of IP Multicast Forwarding within the VLAN Before and After IGMP Snooping Is Run on the Layer-2 Device



Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

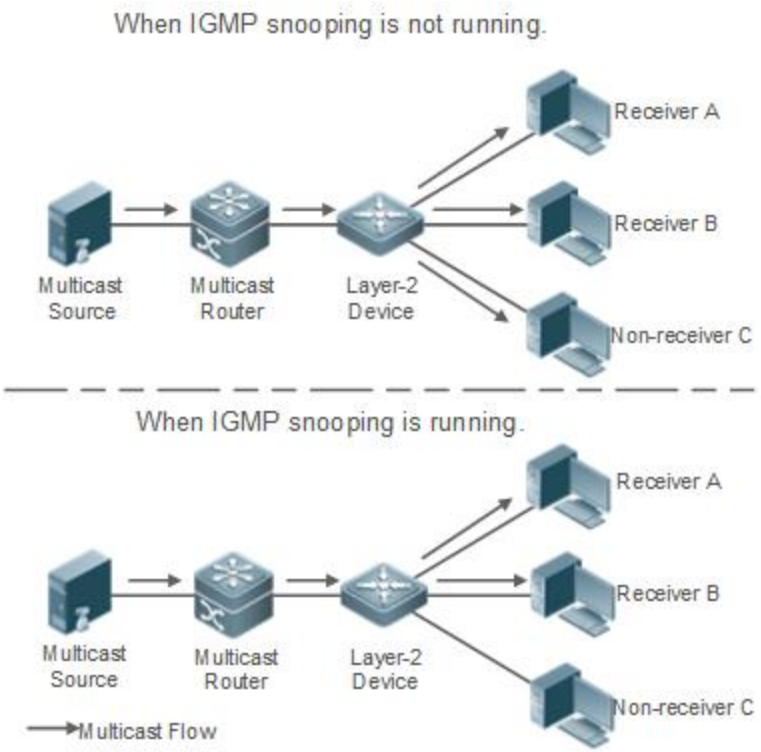
2.2 Applications

Application	Description
Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Shared Multicast Services (Multicast VLAN)	Multiple users can share the multicast traffic of the same VLAN.
Premium Channels and Preview	Controls the range of multicast addresses that allow user demanding and allows preview for profiles who are inhibited from demanding.

2.2.1 Layer-2 Multicast Control

Scenario

- As shown in the following figure, multicast packets are transmitted to users through a Layer-2 switch. When Layer-2 multicast control is not performed, namely, when IGMP snooping is not implemented, multicast packets are flooded to all the users including those who are not expected to receive these packets. After IGMP snooping is implemented, the multicast packets from an IP multicast profile will no longer be broadcast within the VLAN but transmitted to designated receivers.
- Figure 2-2 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



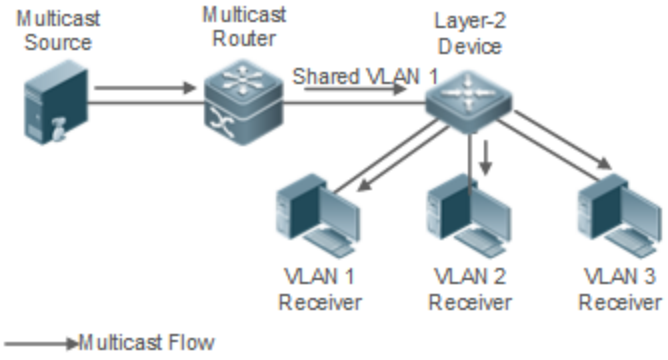
Deployment

- Configure basic IGMP snooping functions.

2.2.2 Shared Multicast Services (Multicast VLAN)

Scenario

- In Shared VLAN Group Learning (SVGL) mode or IVGL-SVGL mode (IVGL: Independent VLAN Group Learning), a device running IGMP snooping can provide shared multicast services (or multicast VLAN services) to the VLAN users. Typically, this function is used to provide the same video-on-demand (VOD) services to multiple VLAN users.
- The following figure shows the operation of a Layer-2 multicast device in SVGL mode of IGMP snooping. The multicast router sends a multicast packet to VLAN 1, and the Layer-2 multicast device automatically transfers the packet to VLAN 1, VLAN 2, and VLAN 3. In this way, the multicast services of VLAN 1 are shared by VLAN 2 and VLAN 3.
- Figure 2-3 Networking Topology of Shared Multicast Services (Multicast VLAN)



If the Layer-2 multicast device operates in IVGL mode, the router must send a packet to each VLAN, which wastes bandwidth and burdens the Layer-2 multicast device.

Deployment

- Configure basic IGMP snooping functions (in SVGL mode or IVGL-SVG mode).

2.2.3 Premium Channels and Preview

Scenario

- In VOD application, by limiting the range of the multicast addresses that a user host can access, unpaid users will not be able to watch the premium channels. Thereafter, the preview service is offered to unpaid users before they decide whether to pay for it.
- The users can preview a premium channel for a certain period of time (for example 1 minute) after demanding it.

Deployment

- Configure basic IGMP snooping functions (in any working mode).
- Configure the range of multicast addresses that a user can access.
- Enable the preview function for VOD profiles that are denied access.

2.3 Features

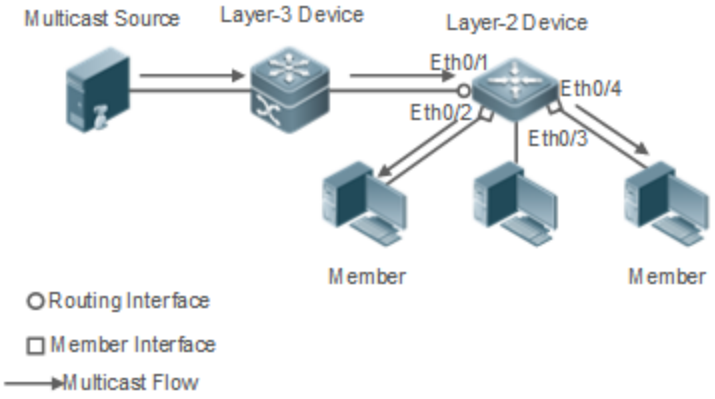
Basic Concepts

Multicast Router Ports and Member Ports

IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

The device running IGMP snooping identifies the ports within the VLAN as a multicast router port or member port so as to manage and control the forwarding of IP multicast traffic within the VLAN. As shown in the following figure, when IGMP snooping is run on a Layer-2 device, multicast traffic enters the multicast router port and exits from the member ports.

Figure 2-4 Networking Topology of Two IGMP Snooping Ports



- Multicast router port: The location of the multicast source is directed by the port on the Layer-2 multicast device which is connected to the multicast router (Layer-3 multicast device): By listening to IGMP packets, the Layer-2 multicast device can automatically detect the multicast router port and maintain the port dynamically. It also allows users to configure a static router port.
- Member port: The port is on a Layer-2 multicast device and is connected to member hosts. It directs the profile members. It is also called the Listener Port. By listening to IGMP packets, the Layer-2 multicast device can automatically detect the member port and maintain the port dynamically. It also allows users to configure a static member port.

Overview

Feature	Description
Listening to IGMP Packets	Discovers and identifies the router port and member port to establish and maintain the IGMP snooping forwarding entries. :
IGMP Snooping Working Modes	Provides independent or shared multicast services to the user VLAN.
Multicast Security Control	Controls the multicast service scope and load to prevent illegal multicast traffic.
Profile	Defines the range of multicast addresses that permit or deny user requests for reference of other functions.
Handling QinQ	Sets the forwarding mode of multicast packets on the QinQ interface.

IGMP Querier	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.

2.3.1 Listening to IGMP Packets

A device running IGMP snooping analyzes IGMP packets received, and finds and identifies the router port and member port using these packets, thereby creating and maintaining an IGMP snooping entry.

Working Principle

A device running IGMP snooping can identify and handle the following types of IGMP packets:

Query Packets

An IGMP querier periodically sends General Query packets. When the IGMP querier receives Leave packets, it sends Group-Specific Query packets.

When the device running IGMP snooping receives the Query packets, it performs the following operations within the VLAN:

- Forward the IGMP Query packets to all the ports (except the receiving port of these packets).
- If the receiving port is a dynamic router port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- If the receiving port is not a dynamic router port, use it as a dynamic router port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- For general queries, reset the aging timer for all the dynamic member ports. If the timer expires, the port will no longer be used as the dynamic member port for the general group. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- For designated query packets, reset the aging timer for all the dynamic member ports of the designated profile. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- If dynamic router port learning is disabled, IGMP snooping will not learn the dynamic router port.

Report Packets

When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a profile, it will also send a report.

By default, IGMP Snooping is capable of processing IGMPv1 and IGMPv2 packets.

When the device running IGMP snooping receives the Report packets, it performs the following operations within the VLAN:

- Forward the Report packets from all the router ports. After the **ip igmp snooping suppression enable** command is run in one IGMP query cycle, only the first report received by each profile will be forwarded.

- If the port on which Report packets are received is a dynamic member port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.
- If the port on which Report packets are received is not a dynamic member port, use it as a dynamic member port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.

Leave Packets

If a host requests to leave a profile, it will send a Leave packet.

When the device running IGMP snooping receives the Leave packets, it performs the following operations within the VLAN:

- Forward the leave packets from all the router ports.
- If the port on which leave packets are received is a dynamic member port and the Leave function is enabled, the port will be immediately deleted from the IGMP snooping forwarding entry of the designated profile and will no longer be used as the dynamic member port.
- If the port on which the leave packets are received is a dynamic member port and the Leave function is disabled, the port state should be maintained.

Related Configuration

Configuring a Static Router Port

Run the **ip igmp snooping vlan mrouter interface** command to configure a static router port.

Configuring a Static Member Port

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

Enabling Report Suppression

Report suppression is disabled by default.

Run the **ip igmp snooping suppression enable** command to enable report suppression.

After report suppression is enabled, in one IGMP query cycle, only the first Report packet received by each profile will be forwarded. The source media access control (MAC) address of the forwarded report will be changed to the MAC address of the device.

Enabling Immediate Leave

Immediate leave is disabled by default.

Run the **ip igmp snooping fast-leave enable** command to enable immediate leave.

Enabling Dynamic Router Port Learning

Dynamic router port learning is enabled by default.

Run the **no ip igmp snooping mrouter learn pim-dvmrp** command to disable dynamic router port learning.

Run the **no ip igmp snooping vlan** *vid* **mrouter learn pim-dvmrp** command to disable dynamic router port learning for designated VLANs.

Configuring the Aging Time of a Dynamic Router Port

The default aging time is 300s.

When a dynamic router port receives a query packet, the aging timer of the port is enabled or reset; if the aging time is not configured, the maximum response time carried by the query packet is used as the aging time.

Run **ip igmp snooping dyn-mr-aging-time** to configure the aging time of the dynamic router port.

Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a query packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time carried by the query packet.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

2.3.2 IGMP Snooping Working Modes

A device running in the three modes (IVGL, SVGL, and IVGL-SVGL) of IGMP snooping can provide independent multicast services or shared multicast services to the user VLAN.

Working Principle

IVGL

In IVGL mode, a device running IGMP snooping can provide independent multicast services to each user VLAN.

Independent multicast services indicate that multicast traffic can be forwarded only within the VLAN it belongs to, and a user host can subscribe to the multicast traffic within the VLAN that the host belongs to.

SVGL

In SVGL mode, a device running IGMP snooping can provide shared multicast services to the user VLAN.

Shared multicast services can be provided only on shared VLANs and sub VLANs and SVGL multicast addresses are used. In a shared VLAN, the multicast traffic within the range of SVGL multicast addresses is forwarded to a sub VLAN, and the user hosts within the sub VLAN subscribe to such multicast traffic from the shared VLAN.

- In a shared VLAN and sub VLAN, shared multicast services will be provided to the multicast traffic within the range of SVGL multicast addresses. Other multicast traffic will be discarded.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.

When the user VLAN is set to a shared VLAN or sub VLAN, shared multicast services are provided; when a user VLAN is set to other VLANs, independent multicast services are provided.

IVGL-SVGL

IVGL-SVGL mode is also called the hybrid mode. In this mode, a device running IGMP snooping can provide both shared and independent multicast services to the user VLAN.

- In a shared VLAN and sub VLAN, multicast services will be provided to the multicast traffic within an SVGL profile. For other multicast traffic, independent multicast services will be provided.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.

When a user VLAN is configured as a shared VLAN or sub VLAN, both public multicast services and independent multicast services available. When a user VLAN is configured as a VLAN other than shared VLAN and sub VLAN, only the independent multicast services are available.

Related Configuration

Enabling IGMP Snooping and Selecting a Working Mode

IGMP snooping is disabled by default.

Run the **ip igmp snooping ivgl** command to enable IGMP snooping in IVGL mode.

Run the **ip igmp snooping svgl** command to enable IGMP snooping in SVGL mode.

Run the **ip igmp snooping ivgl-svgl** command to enable IGMP snooping in IVGL-SVGL mode.

A working mode must be designated when enabling IGMP snooping, namely, one of the preceding working modes must be selected.

Configuring Shared VLAN

The shared VLAN is VLAN 1 by default.

Run the **ip igmp snooping svgl vlan** command to designate a VLAN as the shared VLAN.

In SVGL mode and IVGL-SVGL mode, only one VLAN can be configured as the shared VLAN.

Configuring Sub VLAN

By default, a sub VLAN is any VLAN except the shared VLAN.

Run the **ip igmp snooping svgl subvlan** command to designate a VLAN as the sub VLAN.

In SVGL mode and IVGL-SVGL mode, the number of sub VLANs is not limited.

Configuring an SVGL Profile

No default setting.

Run the **ip igmp snooping svgl profile** *profile_num* command to configure the address range of an SVGL profile.

⚠ In SVGL mode and IVGL-SVGL mode, the SVGL profile range must be configured; otherwise, shared multicast services cannot be provided.

2.3.3 IGMP Security Control

A device running IGMP snooping can control the multicast service scope and load, and effectively prevents illegal multicast traffic.

Working Principle

Configuring the Profile Filtering for User Demanding

By configuring the profile list that a user can access, you can customize the multicast service scope to guarantee the interest of operators and prevent illegal multicast traffic.

To enable this function, you should use a profile to define the range of multicast addresses that a use is allowed to access.

- When the profile is applied on a VLAN, you can define the multicast addresses that a user is allowed to access within the VLAN.
- When the profile is applied on an interface, you can define the multicast addresses that a user is allowed to access under the port.

Multicast Preview

If the service provider wants to allow the users to preview some multicast video traffic that denies the users' access, and stop the multicast video traffic after the preview duration is reached, the user-based multicast preview function should be provided. The multicast preview function is used together with multicast permission control. For example, in the application of videos, the administrator controls some premium channels by running the **ip igmp profile** command on a port or VLAN. In this way, unsubscribed users will not be able to watch these channels on demand. If users want to preview the channels before they decide whether to pay for watching or not, the multicast preview function can be enabled, allowing the premium channels to be previewed by unpaid users for a certain period of time (for example 1 minute).

Controlling the Maximum Number of Profiles Allowed for Concurrent Request

If there is too much multicast traffic requested at the same time, the device will be severely burdened. Configuring the maximum number of profiles allowed for concurrent request can guarantee the bandwidth.

- You can limit the number of profiles allowed for concurrent request globally.
- You can also limit the number of profiles allowed for concurrent request on a port.

Related Configuration

Configuring the Profile Filtering

By default, profiles are not filtered and allow user access.

To filter multicast profiles, run the **ip igmp snooping filter** command in interface configuration mode or global configuration mode.

Enabling Preview

Preview is not enabled by default.

Run the **ip igmp snooping preview** command to enable preview and restrict the range of the profiles permitted for multicast preview.

Run the **ip igmp snooping preview interval** to set the multicast preview duration.

Configuring the Maximum Number of Profiles Allowed for Concurrent Request on a Port

By default, the number of profiles allowed for concurrent request is not limited.

Run the **ip igmp snooping max-groups** command to configure the maximum number of profiles allowed for concurrent request.

Configuring the Maximum Number of Multicast Profiles Allowed Globally

By default, the maximum number of multicast profiles allowed globally is 65,536.

Run the **ip igmp snooping l2-entry-limit** command to configure the maximum number of multicast profiles allowed globally.

2.3.4 IGMP Profile

A multicast profile is used to define the range of multicast addresses that permit or deny user demanding request for reference of other functions.

Working Principle

The profile is used to define the range of multicast addresses.

When SVGL mode is enabled, an SVGL profile is used to define the range of SVGL multicast addresses.

When the multicast filter is configured on an interface, a profile is used to define the range of multicast addresses that permit or deny user request under the interface.

When a VLAN filter is configured, a profile is used to define the range of multicast addresses that permit or deny user request under within the VLAN.

When the preview function is enabled, a profile is used to define the range of multicast address allowed for preview.

Related Configuration

Configuring a Profile

Default configuration:

- Create a profile, which is **deny** by default.

Configuration steps:

- Run the **ip igmp profile** *profile-number* command to create a profile.
- Run the **range** *low-address high_address* command to define the range of multicast addresses. Multiple address ranges are configured for each profile.

- (Optional) Run the **permit** or **deny** command to permit or deny user request (**deny** by default). Only one **permit** or **deny** command can be configured for each profile.

2.3.5 IGMP QinQ

Working Principle

On a device with IGMP snooping enabled and dot1q-tunnel (QinQ) port configured, IGMP snooping will handle the IGMP packets received by the QinQ port using the following two approaches:

- Approach 1: Create a multicast entry on the VLAN where IGMP packets are located. The forwarding of IGMP packets on the VLAN where these packets are located is called transparent transmission. For example, presume that IGMP snooping is enabled for a device, Port A is designated as the QinQ port, the default VLAN of this port is VLAN 1, and it allows the passage of VLAN 1 and VLAN 10 packets. When a multicast Query packet is sent by VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 10 and forwards the multicast Query packet to the router port of VLAN 10.
- Approach 2: Create a multicast entry on the default VLAN of the QinQ port. Encapsulate the multicast packet with the VLAN tag of the default VLAN where the QinQ port is located and forward the packet within the default VLAN. For example, presume that IGMP snooping is enabled for a device, Port A is designated as the QinQ port, the default VLAN of this port is VLAN 1, and it allows the passage of VLAN 1 and VLAN 10 packets. When a multicast Query packet is sent by VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 1, encapsulates the multicast query packet with the tag of VLAN 1, and forward the packet to VLAN 1 router port.

Related Configuration

↘ Configuring QinQ

By default, IGMP snooping works in the mode specified in Approach 2.

Run the **ip igmp snooping tunnel** command to implement Approach 1.

2.3.6 IGMP Querier

On a network with a Layer-3 multicast device, the Layer-3 multicast device acts as an IGMP querier. In this case, a Layer-2 device needs only to listen to IGMP packets to establish and maintain the forwarding entry, realizing Layer-2 multicast.

On a network without a Layer-3 multicast device, the Layer-2 multicast device must be configured with the IGMP querier function so that the device can listen to IGMP packets. In this case, a Layer-2 device needs to act as an IGMP querier as well as listen to IGMP packets to establish and maintain the forwarding entry to realize Layer-2 multicast.

Working Principle

A Layer-2 device acts as an IGMP querier to periodically send IGMP Query packets, listen to and maintain the IGMP Report packets replied by a user, and create a Layer-2 multicast forwarding entry. You can adjust relevant parameters of the Query packets sent by the IGMP querier through configuration.

When the device receives a Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP) packet, it considers that a multicast router, which will act as an IGMP querier, exists on the network and disables the querier function. In this way, IGMP routing will not be affected.

When the device receives the IGMP Query packets from other devices, it will compete with other devices for the IGMP querier.

Enabling the Querier Function

You can enable the querier for a specific VLAN or all VLANs.

Only when the global querier function is enabled can the queriers for specific VLANs take effect.

Specifying the IGMP Version for a Querier

The version of IGMP used for sending Query packets can be configured as IGMPv1, IGMPv2.

Configuring the Source IP Address of a Querier

You can configure the source IP address of a query packet sent by the querier based on VLANs.

When the source IP address of the querier is not configured, the querier will not take effect.

Configuring the Query Interval of a Querier

You can configure the intervals for sending global Query packets based on different queriers on different VLANs.

Configuring the Maximum Response Time of a Query Packet

You can configure the maximum response time carried by a Query packet that is sent by a querier. As IGMP v1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1. You can configure different maximum response time for queriers on different VLANs.

Configuring the Aging Time of a Querier

When other IGMP queriers exist on a network, the existing device will compete with other queriers. If the existing device fails to be elected and is in the non-querier state, the aging timer of a querier will be enabled. After the timer expires, other queriers on the network are considered as expired and the existing device will be resumed as the querier.

Related Configuration

Enabling the Querier Function

By default, the querier function of a device is disabled.

Run the **ip igmp snooping querier** command to enable the global querier function.

Run the **ip igmp snooping vlan** *num* **querier** command to enable the querier function for specific VLANs.

Specifying the IGMP Version for a Querier

By default, a querier runs IGMPv2.

Run the **ip igmp snooping querier version** command to configure the global querier version.

Run the **ip igmp snooping vlan querier version** command to specify the querier version for specific VLANs.

Configuring the Source IP Address of a Querier

By default, the source IP address of a querier is 0.

Run the ip igmp snooping querier address command to enable global source IP addresses of queriers.

Run the ip igmp snooping vlan querier address command to specify the source IP addresses of the queriers on specific VLANs.

Configuring the Query Interval of a Querier

By default, the query interval of a querier is 60s.

Run the **ip igmp snooping querier query-interval** command to enable the global query interval of queriers.

Run **ip igmp snooping vlan querier query-interval** to specify the global query interval of the queriers on specific VLANs.

Configuring the Maximum Response Time of a Query Packet

By default, the maximum response time of a query packet is 10s.

Run the **ip igmp snooping querier max-response-time** command to configure the maximum response time of the query packets sent by global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to specify the maximum response time of the query packets sent by the queriers on specific VLANs.

Configuring the Aging Time of a Querier

By default, the aging time of a querier is 125s.

Run the **ip igmp snooping querier max-response-time** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to configure the aging time of queriers on specific VLANs.

2.4 Configuration

Configuration	Description and Command	
Configuring Basic IGMP Snooping Functions (IVGL Mode)	⚠ Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL mode.	
	ip igmp snooping ivgl	Enables global IGMP snooping in IVGL mode.
	no ip igmp snooping vlan *num*	Disables IGMP snooping for a VLAN.
Configuring Basic IGMP Snooping Functions (SVGL	⚠ Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in SVGL mode.	

Mode)	**ip igmp snooping svgl**	Enables global IGMP snooping in IVGL mode.
	no ip igmp snooping vlan *num*	Disables IGMP snooping for a VLAN.
	ip igmp snooping svgl profile *profile_num*	Configures the SVGL profile.
	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.
	ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.
Configuring Basic IGMP Snooping Functions (IVGL-SVGL Mode)	Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL-SVGL mode.	
	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.
	no ip igmp snooping vlan *num*	Disables IGMP snooping for a VLAN.
	ip igmp snooping svgl profile *profile_num*	Configures the SVGL profile.
	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.
	ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.
Configuring the Packet Processing	(Optional) It is used to adjust relevant configurations for processing protocol packets.	
	ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-id*	Configures a static router port.
	p igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*	Configures a static member port.
	ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**	Enables dynamic router port learning.
	ip igmp snooping dyn-mr-aging-time *time*	Configures the aging time of a dynamic router port.
	ip igmp snooping host-aging-time *time*	Configures the aging time of a dynamic member port.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	ip igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet.
	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.
Configuring IGMP Security Control	(Optional) It used to guarantee the security when a user requests a multicast profile.	
	ip igmp snooping filter *profile-number*	Configures the profile filtering for user access.
	ip igmp snooping vlan *num* **filter** *profile-number*	Configures the per-VLAN profile filtering for user access.
	ip igmp snooping l2-entry-limit *number*	Configures the maximum number of profiles globally for user access.

	ip igmp snooping max-groups *number*	Configures the maximum number of dynamic profiles for user access.
	ip igmp snooping preview *profile-number*	Enables the preview function for a specified profile.
	ip igmp snooping preview interval *num*	Configures the preview duration.
Configuring an IGMP Profile	(Optional) It is used to define the range of multicast addresses that permits or denies the access of a user host.	
	ip igmp profile *profile-number*	Creates a profile.
	range *low-address high_address*	Configures the profile range.
	permit	Permits the access of a user host.
	deny	Denies the access of a user host.
Configuring IGMP QinQ	(Optional) It is used to configure QinQ interface to forward multicast packets using the VLAN identifier (VID) carried by packets.	
	ip igmp snooping tunnel	Configures QinQ to transmit IGMP packets transparently.
Configuring an IGMP Querier	(Optional) It is used to enable IGMP querier function on a network without a Layer-3 multicast device.	
	ip igmp snooping querier	Enables global querier function.
	ip igmp snooping vlan *num* **querier**	Enables the querier for a VLAN.
	ip igmp snooping querier version *num*	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan *num* **querier version** *num*	Specifies the IGMP version for a querier of a VLAN.
	ip igmp snooping querier address a.b.c.d	Configures the source IP address of queriers globally.
	ip igmp snooping vlan *num* **querier address** a.b.c.d	Configures the source IP address for a querier of a VLAN.
	ip igmp snooping querier query-interval *num*	Configures the query interval of queriers globally.
	ip igmp snooping vlan *num* **querier query-interval** *num*	Configures the query interval for a querier of a VLAN.
	ip igmp snooping querier max-response-time *num*	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan *num* **querier max-response-time** *num*	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry *num*	Configures the aging timer for queriers globally.

	ip igmp snooping vlan *num* **querier timer expiry** *num*	Configures the aging timer for a querier of a VLAN.

2.4.1 Configuring Basic IGMP Snooping Functions (IVGL Mode)

Configuration Effect

- Enable IGMP snooping to realize Layer-2 multicast.
- Provide independent multicast services to each VLAN.

Notes

- IP multicast cannot be realized in SVGL mode. If IP multicast must be used, select the IVGL mode.

Configuration Steps

↘ Enabling Global IGMP Snooping in IVGL Mode

Mandatory.

After IGMP snooping is enabled globally, this function will be enabled for all VLANs.

If not specified, it is advised to run global IGMP snooping on all the devices connected user hosts.

↘ Disabling IGMP Snooping for a VLAN

(Optional) You can use this function if you wish to disable IGMP snooping on specified VLANs.

Only when global IGMP snooping is enabled can it be disabled on specified VLANs.

In IVGL mode, each VLAN can enjoy independent multicast services. Disabling any VLAN multicast services will not interfere in the services provided to the others.

Verification

- Run the **show ip igmp snooping gda-table** command to display the IGMP snooping forwarding table and verify that the member ports include only those connecting member hosts.
- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL mode.

Related Commands

↘ Enabling Global IGMP Snooping in IVGL Mode

Command	**ip igmp snooping ivgl**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on all VLANs.

	By default, IGMP snooping is disabled.

Disabling IGMP Snooping for a VLAN

Command	**no ip igmp snooping vlan** *num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Only when global IGMP snooping is enabled can it be disabled on specified VLANs. In IVGL mode, you can disable IGMP snooping on any VLAN.

Displaying the IGMP Snooping Entry

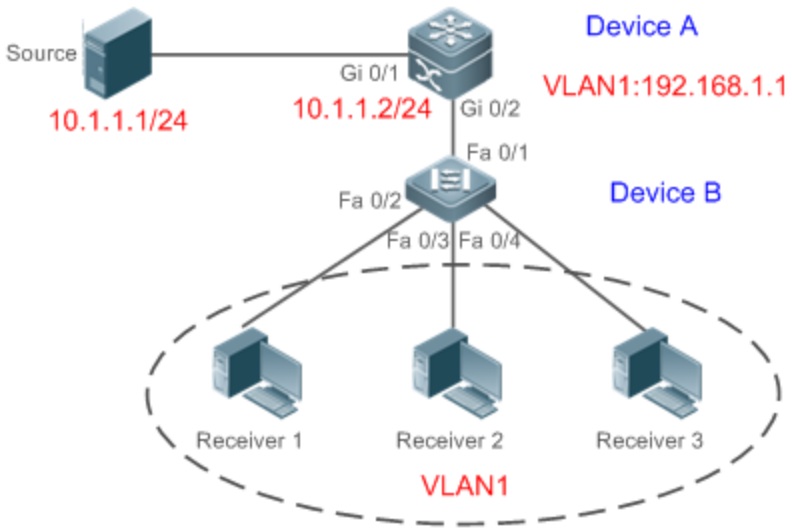
Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

Displaying the IGMP Snooping Working Mode

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL mode, the following information is displayed: `IGMP Snooping running mode: IVGL`

Configuration Example

Providing Layer-2 Multicast Services for the Subnet Hosts

Scenario **Figure 2-5**	
	A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1, Receiver 2, and Receiver 3 belong to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode.

A	`A# configure terminal`
	`A(config)# ip multicast-routing`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode`
	`A(config-if-GigabitEthernet 0/1)# exit`
	`A(config)# interface vlan 1`
	`A(config-if-VLAN 1)# ip pim sparse-mode`
	`A(config-if-VLAN 1)# exit`

B	`B# configure terminal` `B(config)# ip igmp snooping ivgl`
Verification	Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G. ● Confirm that the packets (10.1.1.1 and 229.1.1.1) are received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the port (10.1.1.1, 229.1.1.1, 1) includes only Fa0/2. ● Check whether the IGMP snooping working mode is IVGL.
B	`B# show ip igmp snooping gda-table`

```
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(D)
```

```
B# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

Common Errors

- The working mode of IGMP snooping is improper.

2.4.2 Configuring Basic IGMP Snooping Functions (SVGL Mode)

Configuration Effect

- Enable IGMP snooping and select SVGL mode to realize Layer-2 multicast.
- Share the VLAN multicast services.

Configuration Steps

Enabling Global IGMP Snooping in SVGL Mode

Mandatory.

Enable global IGMP snooping in SVGL mode.

Configure the range of associated SVGL profiles.

Specifying the SVGL Shared VLAN

(Optional) By default, VLAN 1 is used as the shared VLAN. You can adjust this configuration for other options.

Specifying the SVGL Sub VLAN

(Optional) By default, all the VLANs are used as the sub VLANs of SVGL and can share the multicast services of the shared VLAN. You can adjust this configuration for other options.

Verification

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in SVGL mode.
- Run the **show ip igmp snooping gda-table** command to check whether inter-VLAN multicast entries are properly formed.

Related Commands

Enabling Global IGMP Snooping in SVGL Mode

Command	ip igmp snooping svgl
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the SVGL mode is selected, the range of profiles within SVGL multicast addresses needs to be associated.

Configuring the SVGL profile

Command	**ip igmp snooping svgl profile** *profile_num*
Parameter Description	*profile_num:* Configures SVGL to associate a profile.
Command Mode	Global configuration mode
Usage Guide	By default, no profile is associated with SVGL.

Specifying the SVGL Shared VLAN

Command	**ip igmp snooping svgl vlan** *vid*
Parameter Description	*vid*: Indicates a VLAN.
Command Mode	Interface configuration mode
Usage Guide	By default, VLAN 1 is used as the shared VLAN.

Specifying the SVGL Sub VLAN

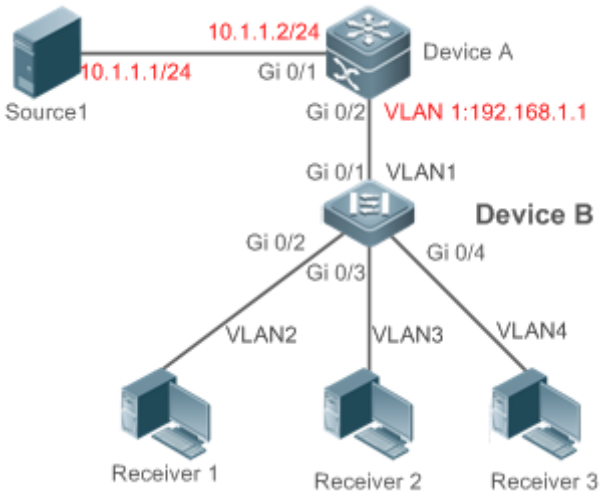
Command	**ip igmp snooping svgl subvlan** *vid-range*
Parameter Description	*vid-range*: Indicates VLAN ID or the range of VLAN IDs.
Command Mode	Interface configuration mode
Usage Guide	By default, all the VLANs except the shared VLAN are used as sub VLANs.

Displaying the IGMP Snooping Working Mode

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in SVGL mode, the following information is displayed: `IGMP Snooping running mode: SVGL`

Configuration Example

Enabling SVGL on the Access Device

Scenario **Figure 2-6**	
	A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1 is connected to VLAN 2, Receiver 2 is connected to VLAN 3, and Receiver 3 is connected to VLAN 4.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select SVGL mode. ● Configure the range of associated SVGL multicast addresses on B.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping svgl B(config)#ip igmp snooping svgl profile 1

Verification	Send packets from the source (10.1.1.1) to G (229.1.1.1) and add Receiver 1, Receiver 2 and Receiver 3 to G. ● Confirm that the packets (10.1.1.1 and 224.1.1.1) are received by Receiver 1, Receiver 2, and Receiver 3. ● Display the IGMP snooping forwarding entry on B and ensure that the ports (*, 224.1.1.1, 1) include Gi0/2, Gi0/3, and Gi0/4. ● Check whether the IGMP snooping working mode is SVGL.
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D) B# show ip igmp snooping IGMP Snooping running mode: SVGL IGMP Snooping L2-entry-limit: 65536 SVGL vlan: 1 SVGL profile number: 1 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds)

	Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Common Errors

- The SVGL profile is not configured.
- The sent multicast traffic is not within the SVGL profile.

2.4.3 Configuring Basic IGMP Snooping Functions (IVGL-SVGL Mode)

Configuration Effect

- Enable IGMP snooping and select IVGL-SVGL mode to realize Layer-2 multicast.
- The SVGL profiles can share the multicast services.
- The non-SVGL profiles run in IVGL mode.

Configuration Steps

Enabling Global IGMP Snooping in IVGL-SVGL Mode

Mandatory.

Enable global IGMP snooping in IVGL-SVGL mode.

Configure the range of associated SVGL profiles.

Specifying the SVGL Shared VLAN

(Optional) By default, VLAN 1 is used as the shared VLAN. You can adjust this configuration for other options.

Specifying the SVGL Sub VLAN

(Optional) By default, all the VLANs are used as the sub VLANs of SVGL and can share the multicast services of the shared VLAN. You can adjust this configuration for other options.

Verification

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL-SVGL mode.
- Run the **show ip igmp snooping gda-table** command to check whether inter-VLAN multicast entries are properly formed for the SVGL profiles.
- Run the **show ip igmp snooping gda-table** command to check whether intra-VLAN multicast entries are properly formed for the SVGL profiles.

Related Commands

Enabling Global IGMP Snooping in IVGL-SVGL Mode

Command	**ip igmp snooping ivgl-svgl**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the IVGL-SVGL mode is selected, the SVGL profiles needs to be associated.

Configuring the SVGL Profile

Command	**ip igmp snooping svgl profile** *profile_num*
Parameter Description	*profile_num:* Configures SVGL to associate a profile.
Command Mode	Global configuration mode
Usage Guide	By default, no profile is associated with SVGL.

Specifying the SVGL Shared VLAN

Command	**ip igmp snooping svgl vlan** *vid*
Parameter Description	*vid*: Indicates a VLAN.
Command Mode	Interface configuration mode
Usage Guide	By default, VLAN 1 is used as the shared VLAN.

Specifying the SVGL Sub VLAN

Command	**ip igmp snooping svgl subvlan** *vid-range*
Parameter Description	*vid-range*: Indicates VLAN ID or the range of VLAN IDs.
Command Mode	Interface configuration mode
Usage Guide	By default, all the VLANs except the shared VLAN are used as sub VLANs.

Displaying the IGMP Snooping Working Mode

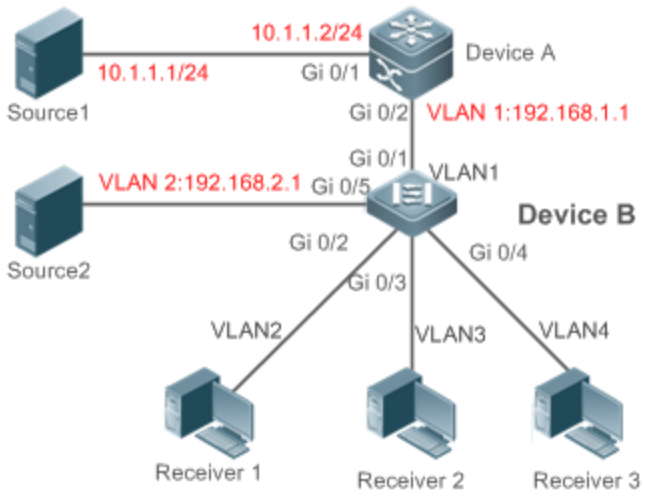
Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in SVGL mode, the following information is displayed: `IGMP Snooping running mode: SVGL`

Displaying the IGMP Snooping Working Mode

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL-SVGL mode, the following information is displayed: `IGMP Snooping running mode: IVGL-SVGL`

Configuration Example

Enabling IVGL-SVGL on the Access Device

Scenario Figure 2-7	
	A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1 is connected to VLAN 2, Receiver 2 is connected to VLAN 3, and Receiver 3 is connected to VLAN 4.
Configuration Steps	● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL-SVGL mode. ● Configure the range of associated SVGL multicast addresses on B.

A	`A# configure terminal`
	`A(config)# ip multicast-routing`
	`A(config)# interface GigabitEthernet 0/1`

	A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping ivgl-svgl B(config)#ip igmp snooping svgl profile 1
Verification	Send packets from Source 1 (10.1.1.1) to G (224.1.1.1) and add Receiver 1, Receiver 2 and Receiver 3 to G. Send packets from Source 2 (192.168.2.1) to the destination (239.1.1.1) and add Receiver 1 239.1.1.1. ● Confirm that the packets (10.1.1.1 and 224.1.1.1) are received by Receiver 1, Receiver 2, and Receiver 3. ● Check that packets (192.168.2.1 and 239.1.1.1) can be received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the ports (*, 224.1.1.1, 1) include Gi0/2, Gi0/3, and Gi0/4, and the port (*, 239.1.1.1, 1) is Gi0/2. ● Check whether the IGMP snooping working mode is IVGL-SVGL.
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D)

```
(*,239.1.1.1, 2):
  VLAN(2) 1 OPORTS:
GigabitEthernet 0/2(D)
```

```
B# show ip igmp snooping
IGMP Snooping running mode: IVGL-SVGL
IGMP Snooping L2-entry-limit: 65536
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

Common Errors

- The SVGL profile is not configured.
- The sent multicast traffic is not within the SVGL profile.
- The IVGL multicast traffic cannot be forwarded within the SVGL profile.

2.4.4 Configuring the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all profiles.

- Configure specified ports as the static member ports to receive the multicast traffic from specified profiles
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or profile to the router port within a query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network.
- Configure the immediate-leave function to delete a port from the entry of member ports when a leave packet is received by the port.
- Disable dynamic router port learning to disable the learning of any router port.
- Based on network load and configuration of a multicast device, you can adjust the aging time of a router port and member port as well as the maximum response time of a query packet.

Notes

- Only when basic IGMP snooping is configured can relevant configurations take effect.

Configuration Steps

Configuring a Static Router Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive all the multicast traffic within the VLAN.

Configuring a Static Member Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive specific multicast traffic within the VLAN.

Enabling Report Packet Suppression

- Optional.
- When there are numerous receivers to receive the packets from the same multicast profile, you can enable Report packets suppression to suppress the number of Report packets to be sent.

Enabling the Immediate-Leave Function

- Optional.
- When there is only one receiver on a port, you can enable Leave to speed up the convergence of protocol upon leave.

Disabling Dynamic Router Port Learning

- Optional.
- This function is used when multicast traffic needs to be forwarded only within the Layer-2 topology but not to a Layer-3 router.

Configuring the Aging Time of a Dynamic Router Port

- Optional.
- You can configure the aging time based on network load.

Configuring the Aging Time of a Dynamic Member Port

- Optional.
- You can configure the aging time based on the interval for sending IGMP query packets by the connected multicast router. Typically, the aging time is calculated as follows: Interval for sending IGMP query packets x 2 + Maximum response time of IGMP packets

Configuring the Maximum Response Time of a Query Packet

- Optional.
- You can configure the aging time based on network load.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

Configuring a Static Router Port

Command	**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	In SVGL mode, if a sub VLAN is not configured, only the configurations for the static router port within the shared VLAN can take effect, and the others can be configured but cannot take effect. If a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL-SVGL mode, if a sub VLAN is not configured, the configurations for the static router ports within all the VLANs can take effect; if a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL mode, the configurations for the static router ports within all the VLANs can take effect.

Configuring a Static Member Port

Command	**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *group-address*: Indicates a profile address. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

Enabling Report Packet Suppression

Command	**ip igmp snooping suppression enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed.

Enabling the Immediate-Leave Function

Command	**ip igmp snooping fast-leave enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets. The immediate-leave function applies only to the scenario where only one host is connected to a device port. It is used to conserve bandwidth and resources.

Enabling Dynamic Router Port Learning

Command	**ip igmp snooping** [**vlan** *vid*] **mrouter learn pim-dvmrp**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A router port is the port that is connected directly to a multicast device running IGMP snooping and a multicast neighbor device running multicast routing protocol. By default, dynamic router port learning is enabled and the device automatically listens to IGMP Query packets, DVMRP packets, and PIM Hello packets.

Configuring the Aging Time of a Dynamic Router Port

Command	**ip igmp snooping dyn-mr-aging-time** *seconds*
Parameter Description	*seconds*: Indicates the aging time of a dynamic router port in the unit of seconds. The value ranges from 1 to 3,600.
Command Mode	Global configuration mode
Usage Guide	If a dynamic router port does not receive an IGMP general query packet or a PIM Hello packet before the aging timer expires, the device will delete this port from the router port entry. When dynamic router port learning is enabled, you can run this command to adjust the aging time of the dynamic router port. If the aging time is too short, the multicast device may frequently add or delete a router port.

Configuring the Aging Time of a Dynamic Member Port

Command	**ip igmp snooping host-aging-time** *seconds*
Parameter Description	*seconds*: Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	The aging time of a dynamic member port indicates the time when a device port receives the IGMP join packet sent from host for subscribing to an IP multicast profile. When the IGMP join packet is received, the aging time of the dynamic member port will be reset. The value of the timer time is host-aging-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. After the aging time is configured, the aging time of following received IGMP join packets will be host-aging-time. This configuration takes effect after the next IGMP join packet is received, and the timer of the port in use will not be refreshed.

Configuring the Maximum Response Time of a Query Packet

Command	**ip igmp snooping query-max-response-time** *seconds*
Parameter Description	*seconds*: Indicates the maximum response time.
Command Mode	Global configuration mode
Usage Guide	When an IGMP general Query packet is received, the multicast device will reset the aging time of all the dynamic member ports, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. When an IGMP profile-specific Query packet is received, the multicast device will reset the aging time of all the dynamic member ports of the specific profile, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will

	delete the port from the entry of IGMP snooping member port. This configuration takes effect after the next Query packet is received, and the timer in use will not be refreshed.

Displaying Router Ports

Command	**show ip igmp snooping mroute**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	If the router port is successfully configured, an "S" will be displayed in the port information.
	`Hostname(config)#show ip igmp snooping mrouter`
	`Multicast Switching Mroute Port`
	`  D: DYNAMIC`
	`  S: STATIC`
	`(*, *, 1):`
	`  VLAN(1)  1 MROUTES:`
	`    GigabitEthernet 0/1(S)`

Displaying the Information of Dynamic Router Port Learning

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Run the **show ip igmp snooping** command to display the aging time and learning status of the dynamic router port.
	`Dynamic Mroute Aging Time : 300(Seconds)`
	`Multicast router learning mode: pim-dvmrp`

Displaying the Information of a Member Port

Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the member port is successfully configured, an "S" will be displayed in the port information.

	Hostname(config)#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/1(S

Displaying Other Parameters

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave. IGMP Fast-Leave: Enable IGMP Report suppress: Enable Query Max Response Time: 20(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

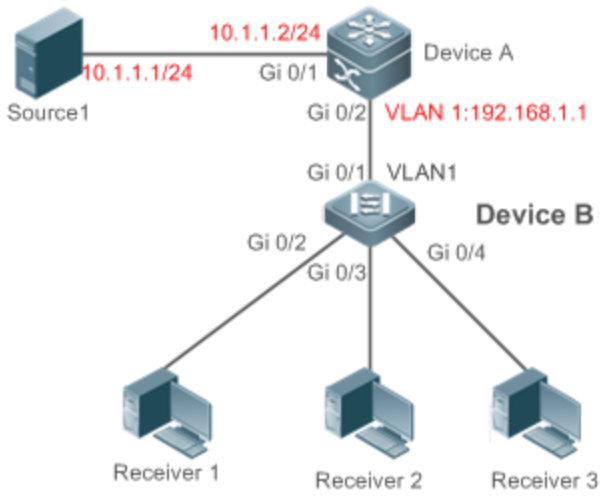
Configuration Example

Configuring a Static Router Port and Static Member Port

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
	Hostname# configure terminal Hostname(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Hostname(config)# end
Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
	Hostname# configure terminal Hostname(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Hostname(config)# end
Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.
	Hostname#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/0(S) Hostname#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/0(SM)

Enabling Report Packet Suppression

Scenario **Figure 2-8**	
	A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode. ● Enable Report packets suppression on B.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable
Verification	Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.

B	B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Configuring Other Parameters

Configuration Steps	• Configure basic IGMP snooping functions. • Enable Immediate-leave function. • Disable router port learning. • Configure the aging time of a router port. • Configuring the aging time of a member port. • Configure the response time of a Query packet.
	Hostname# configure terminal Hostname(config)# ip igmp snooping fast-leave enable Hostname(config)# no ip igmp snooping mrouter learn pim-dvmrp Hostname(config)#ip igmp snooping dyn-mr-aging-time 200 Hostname(config)#ip igmp snooping host-aging-time 100 Hostname(config)#ip igmp snooping query-max-response-time 60 Hostname(config)# end
Verification	Run the **show ip igmp snooping** command to check whether the configuration is successful.
	Hostname#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable

	Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 200(Seconds) Dynamic Host Aging Time : 100(Seconds)

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

2.4.5 Configuring IGMP Security Control

Configuration Effect

- Configure the range of multicast addresses that a user can access.
- Configure to allow a user from an unauthorized profile to preview a multicast channel.
- Configure the number of multicast addresses that a user can access.
- Configure to limit a user to receive only the multicast traffic from a router port to prevent illegal multicast traffic sent by the end user.
- Configure to limit a user to receive only the multicast traffic from designated source IP addresses to prevent illegal multicast traffic.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↘ Configuring the Profile Filtering

- Optional.
- If you want to limit the profile packets to be received by a port, you can configure the profile filtering on the port.
- If you want to limit the multicast packets to be received by a VLAN, you can configure the per-VLAN profile filtering.

↘ Enabling Multicast Preview

- Optional.

- You can enable multicast preview for a user from an unauthorized profile.

Configuring the Maximum Number of Profiles

- Optional.
- If you want to limit the number of multicast profiles that a port is allowed to receive, you can configure the maximum number of multicast profiles allowed for this port.
- If you want to limit the number of multicast profiles that global ports are allowed to receive, you can configure the maximum number of multicast profiles allowed for these ports.

Verification

- Run the **show ip igmp snooping interfaces** command to display the profile filtering and the maximum number of multicast profiles for a port.
- Run the **show ip igmp snooping vlan** command to display the per-VLAN profile filtering.
- Run the **show ip igmp snooping** command to check whether the maximum number of global multicast profiles, preview function, source port inspection, and source IP address inspection take effect.

Related Commands

Configuring the Profile Filtering

Command	**ip igmp snooping filter** *profile-number*
Parameter Description	*profile-number*: Indicates a profile number.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Per-VLAN Profile Filtering

Command	**ip igmp snooping vlan** *vid* **filter** *profile-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *profile-number*: Indicates a profile number.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Profiles on a Port

Command	**ip igmp snooping max-groups** *number*
Parameter Description	*number*: Indicates the maximum number of multicast profiles.
Command Mode	Interface configuration mode

Usage Guide	This value indicates only the number of dynamic multicast profiles, and the number of static profiles is not included. The counter of multicast profiles is based on the VLAN that the port belongs to. For example, if a port belongs to three VLANs, and all three of them receive a request packet from multicast profile 224.1.1.1 simultaneously, then the counter of multicast profiles will be 3 but not 1.

Configuring the Maximum Number of Global Profiles

Command	**ip igmp snooping l2-entry-limit** *number*
Parameter Description	*number*: Indicates the maximum number of multicast profiles.
Command Mode	Global configuration mode
Usage Guide	This value includes the number of both dynamic profiles as well as static profiles.

Enabling Preview

Command	**ip igmp snooping preview** *profile-number*
Parameter Description	*profile number:* Indicates the range of multicast addresses allowed for preview. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Preview Duration

Command	**ip igmp snooping preview interval** *num*
Parameter Description	*num:* Specifies the preview duration which ranges from 1s to 300s (60s by default).
Command Mode	Global configuration mode
Usage Guide	This configuration allows unauthorized users to receive multicast traffic within the preview duration. After the duration is met, the preview will be stopped; the preview can be resumed in 300s.

Displaying the Per-Port Profile Filtering

Command	**show ip igmp snooping interface**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	If the function is configured, the profile will be displayed, for example:
	`Hostname#show ip igmp snooping interfaces gigabitEthernet 0/1`
	`Interface Filter profile number max-group`

	``` ------------------------- --------------------- --------- GigabitEthernet 0/1 1 ```

Displaying the Per-VLAN Profile Filtering

Command	**show ip igmp snooping vlan**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the function is configured, the profile will be displayed, for example: ``` IGMP VLAN filter: 1 ```

Displaying the Maximum Number of Interface Profiles

Command	**show ip igmp snooping interface**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the maximum number of multicast addresses for a port is configures, the value will be displayed, for example: ``` Hostname#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ------------------------- --------------------- --------- GigabitEthernet 0/1 1 200 ```

Displaying the Maximum Number of Global Profiles

Command	**show ip igmp snooping vlan**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the function is configured, the profile will be displayed, for example: ``` IGMP Snooping L2-entry-limit: 65536 ```

Displaying the Information of the Preview Function

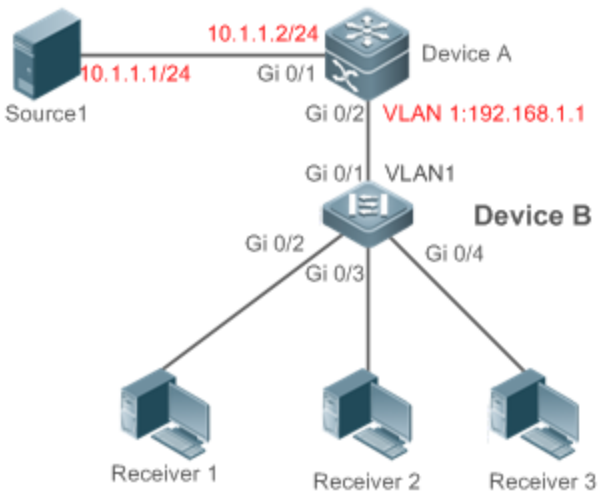
Command	**show ip igmp snooping**
Parameter	N/A

Description	
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	If the range of multicast addresses for a port is configured, preview will be enabled, for example:
	`IGMP Preview: Enable`
	`IGMP Preview group aging time : 60(Seconds)`

Configuration Example

Configuring the Profile Filtering and the Maximum Number of Demanded Profiles

Scenario **Figure 2-9**	
	A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1. By configuring VLAN 1, you can configure to allow the users within VLAN 1 to receive only the profiles whose addresses range from 225.1.1.1 to 225.1.255.255. You can configure Receiver 1 to receive only the profiles whose addresses range from 225.1.1.1 to 225.1.1.255, Receiver 2 to receive only the profiles whose addresses range from 225.1.2.1 to 255.1.2.255, and Receiver 3 to receive only the profiles whose addresses range from 225.1.3.1 to 225.1.3.255. At most 10 profiles can be added to a port and at most 100 profiles can be added globally.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode. ● Configure the range and maximum number of multicast addresses on B.
A	`A# configure terminal` `A(config)# ip multicast-routing`

	A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#rang B(config-profile)#range 225.1.1.1 225.1.255.255 B(config-profile)#exit B(config)#ip igmp profile 2 B(config-profile)#permit B(config-profile)#range 225.1.1.1 225.1.1.255 B(config-profile)#exit B(config)#ip igmp profile 3 B(config-profile)#permit B(config-profile)#range 225.1.2.1 225.1.2.255 B(config-profile)#exit B(config)#ip igmp profile 4 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 225.1.3.1 225.1.3.255 B(config-profile)#exit B(config)#ip igmp snooping l2-entry-limit 100 B(config)#ip igmp snooping vlan 1 filter 1 B(config)#int gigabitEthernet 0/2 Hostname(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 2 Hostname(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10

	B(config)#int gigabitEthernet 0/3 Hostname(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 3 Hostname(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/4 Hostname(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 4 Hostname(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10
Verification	● Run the **show ip igmp snooping interfaces** command to display the profile filtering and the maximum number of multicast profiles for a port. ● Run the **show ip igmp snooping** command to display the maximum number of global multicast groups.
B	B#show ip igmp snooping interfaces Interface Filter profile number max-group ---------- ---------- --------- GigabitEthernet 0/2 2 10 GigabitEthernet 0/3 3 10 GigabitEthernet 0/4 4 10 B#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 100 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

- The multicast router port is not learned, leading to failure to receive the multicast traffic.

2.4.6 Configuring an IGMP Profile

Configuration Effect

- Create an IGMP filtering profile.

Configuration Steps

Creating a Profile

- (Optional) Create an IGMP filtering profile.

Configuring the Profile Range

- (Optional) Configure the range of multicast profile addresses.

Configuring the Profile Filtering

- (Optional) Configure the filtering mode of profile to **permit** or **deny**.

Verification

- Run the **show running-config** command to check whether the preceding configurations take effect.

Related Commands

Creating a Profile

Command	**ip igmp profile** *profile-number*
Parameter Description	*profile-number*: Indicates the number of a profile.
Command Mode	Global configuration mode
Usage Guide	

Configuring the Profile Range

Command	**range** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address*: Specifies the start address. *low-ip-address*: Specifies the end address. Only one address is configured by default.
Command Mode	Profile configuration mode
Usage Guide	You can configure multiple addresses. If the IP addresses of different ranges are consecutive, the addresses will be combined.

Configuring the Profile Filtering

Command	deny
Parameter Description	N/A
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode of profile is set to **deny** while the range of multicast profiles is not specified, no profile is to be denied, which means to permit all profiles.

Configuring the Profile Filtering

Command	permit
Parameter Description	N/A
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode of profile is set to **permit** while the range of multicast profiles is not specified, no profile is to be permitted, which means to deny all profiles.

Configuration Example

Creating a Filtering Profile

Configuration Steps	● Create a filtering profile.
	B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 224.1.1.1 235.1.1.1 B(config-profile)#
Verification	Run the **show running-config** command to check whether the configuration is successful.
	ip igmp profile 1 permit range 224.1.1.1 235.1.1.1 !

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.
- The mode of profile is set to **permit** while the range of multicast profiles is not specified, leading to the denial of all profiles.

2.4.7 Configuring IGMP QinQ

Configuration Effect

- Create a multicast entry on the VLAN where IGMP packets are located. Forward IGMP packets on the VLAN where these packets are located, realizing transparent transmission.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↘ Configuring QinQ Transparent Transmission

- If the QinQ interface needs to forward multicast packets on the VLANs where the VIDs of the packets specify, enable QinQ to realize transparent transmission.

Verification

- Run the **show ip igmp snooping** command to check whether the configuration takes effect.

Related Commands

↘ Configuring QinQ Transparent Transmission

Command	**ip igmp snooping tunnel**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable QinQ to realize transparent transmission of IGMP packets.

↘ Displaying QinQ Configuration

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed. IGMP Tunnel: Enable

Configuration Example

↘ Configuring QinQ Transparent Transmission

Configuration	● Configure basic IGMP snooping functions.

Steps	● Configure QinQ transparent transmission.
	Hostname# configure terminal Hostname(config)# ip igmp snooping tunnel Hostname(config)# Hostname(config)# end
Verification	Run the **show ip igmp snooping** command to check whether the configuration is successful.
	IGMP Tunnel: Enable

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

2.4.8 Configuring an IGMP Querier

Configuration Effect

- Configure the device as an IGMP querier, which will send IGMP Query packets periodically and collect user demanding information.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↘ Enabling the Querier Function

- (Optional) Enable IGMP querier function globally or for a specified VLAN.
- (Optional) Disable the IGMP querier function for a specified VLAN.

↘ Configuring the Source IP Address of a Querier

- (Optional) You can configure the source IP address of a Query packet sent by the querier based on VLANs.
- After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect.

↘ Configuring the Maximum Response Time of a Query Packet

- (Optional) Adjust the maximum response time carried by an IGMP Query packet. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1.

↘ Configuring the Query Interval of a Querier

- (Optional) Adjust the interval of the IGMP querier for sending query packets.

↘ Configuring the Aging Timer of a Querier

- (Optional) Configure the aging timer of other IGMP queriers on the network.

Specifying the IGMP Version for a Querier

- (Optional) Specify the IGMP version for a querier (IGMPv2 by default).

Verification

- Run the **show ip igmp snooping querier detail** command to check whether the configuration takes effect.

Related Commands

Enabling the IGMP Querier Function

Command	**ip igmp snooping** [**vlan** *vid*] **querier**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	IGMP querier for a specified VLAN will take effect only after global IGMP querier is enabled. If global IGMP querier is disabled, IGMP querier for all the VLANs will be disabled.

Configuring the Source IP Address of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *a.b.c.d*: Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect. If the source IP address is specified by a VLAN, the address will be used preferentially.

Configuring the Maximum Response Time of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier max-response-time** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the maximum response time. in the unit of seconds. The value ranges from 1 to 25.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Query Interval of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the query interval in the unit of seconds. The value ranges from 1 to 18,000.

Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Aging Timer of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier timer expiry** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the timeout time in the unit of seconds. The value ranges from 60 to 300.
Command Mode	Global configuration mode
Usage Guide	A device may fail to be elected as the querier even when its querier function is enabled. If a device that fails to be elected does not receive the Query packet sent by the querier in the aging time, the querier in use is considered as expired, and a new round of election will be raised. If the aging time is specified by a VLAN, the value will be used preferentially.

Specifying the IGMP Version for a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier version 1**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A querier can be run in IGMPv1 and IGMPv2 (IGMPv2 by default). You can also run a command to configure the version to IGMPv1. If the IGMP version for a querier is specified by a VLAN, the version will be used preferentially.

Displaying the IGMP Querier Configuration

Command	**show ip igmp snooping querier detail**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

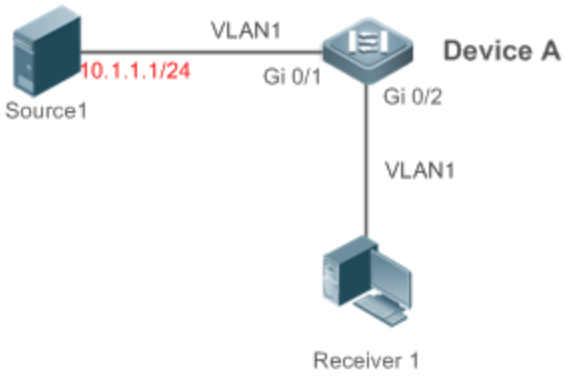
Usage Guide	If QinQ is enabled, the following content is displayed.
	`Hostname(config)#show ip igmp snooping querier detail`
	`Vlan IP Address IGMP Version Port`
	`----------`
	
	`Global IGMP switch querier status`
	`----------`

```
admin state                    : Enable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 125

Vlan 1:   IGMP switch querier status
------------------------------------------------------------
admin state                    : Disable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 125
operational state              : Disable
operational version            : 2
```

Configuration Example

↘ Enabling the IGMP Querier Function

Scenario **Figure 2-10**	
	In the scenario without Layer-3 multicast equipment, the multicast traffic can be forwarded only on the Layer-2 network. A acts as a Layer-2 device to connect to the multicast source and receiver.
Configuration	● Enable global IGMP snooping on A in IVGL mode.

Steps	● Enable IGMP querier for VLAN 1 on A.
A	A(config)#ip igmp snooping ivgl A(config)#ip igmp snooping querier A(config)#ip igmp snooping querier address 10.1.1.1 A(config)#ip igmp snooping vlan 1 querier
Verification	Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.
A	A(config)#show ip igmp snooping querier Vlan IP Address IGMP Version Port --- 1 10.1.1.1 2 switch A(config)#show ip igmp snooping querier vlan 1 Vlan 1: IGMP switch querier status --- elected querier is 10.1.1.1 (this switch querier) --- admin state : Enable admin version : 2 source IP address : 10.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 operational state : Querier operational version : 2

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

2.5 Monitoring

Clearing

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

Description	Command
Clears the statistics on IGMP snooping.	**clear ip igmp snooping statistics**
Clears the dynamic router ports and member ports.	**clear ip igmp snooping gda-table**

Displaying

Description	Command
Displays basic IGMP snooping configurations.	**show ip igmp snooping** [**vlan** *vlan-id*]
Displays the statistics on IGMP snooping.	**show ip igmp snooping statistics** [**vlan** *vlan-id*]
Displays the router ports.	**show ip igmp snooping mrouter**
Displays the IGMP snooping entries.	**show ip igmp snooping gda-table**
Displays the profile.	**show ip igmp profile** [*profile-number*]
Displays the IGMP snooping configurations on an interface.	**show ip igmp snooping interface** *interface-name*
Displays the IGMP querier.	**show ip igmp snooping querier** [**detail**]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs all IGMP Snooping functions.	**debug igmp-snp**
Debugs the IGMP snooping events.	**debug igmp-snp event**
Debugs the IGMP snooping packets.	**debug igmp-snp packet**
Debugs the communications between IGMP snooping and MSF.	**debug igmp-snp msf**
Debugs the IGMP snooping alarms.	**debug igmp-snp warning**

Security Configuration

1. Configuring AAA
2. Configuring RADIUS
3. Configuring TACACS+
4. Configuring 802.1X
5. Configuring Web Authentication
6. Configuring SCC
7. Configuring Global IP-MAC Binding
8. Configuring Password Policy
9. Configuring Storm Control
10. Configuring SSH
11. Configuring CPU Protection
12. Configuring DHCP Snooping
13. Configuring Dynamic ARP Inspection
14. Configuring IP Source Guard

15. Configuring NFPP

1 Configuring AAA

1.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring the authentication, authorization, and accounting services. Devices support the AAA application.

AAA provides the following services in a modular way:

Authentication: Refers to the verification of user identities for network access and network services. Authentication is classified into local authentication and authentication through Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System+ (TACACS+).

Authorization: Refers to the granting of specific network services to users according to a series of defined attribute-value (AV) pairs. The pairs describe what operations users are authorized to perform. AV pairs are stored on network access servers (NASs) or remote authentication servers.

Accounting: Refers to the tracking of the resource consumption of users. When accounting is enabled, NASs collect statistics on the network resource usage of users and send them in AV pairs to authentication servers. The records will be stored on authentication servers, and can be read and analyzed by dedicated software to realize the accounting, statistics, and tracking of network resource usage.

AAA is the most fundamental method of access control. Devices also provide other simple access control functions, such as local username authentication and online password authentication. Compared to them, AAA offers higher level of network security.

AAA has the following advantages:

- Robust flexibility and controllability
- Scalability
- Standards-compliant authentication
- Multiple standby systems

1.2 Applications

Application	Description
Configuring AAA in a Single-Domain Environment	AAA is performed for all the users in one domain.
Configuring AAA in a Multi-Domain Environment	AAA is performed for the users in different domains by using different methods.

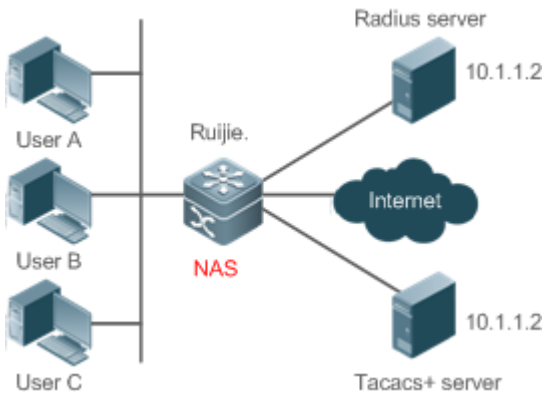
1.2.1 Configuring AAA in a Single-Domain Environment

Scenario

In the network scenario shown in Figure 1-1, the following application requirements must be satisfied to improve the security management on the NAS:

1. To facilitate account management and avoid information disclosure, each administrator has an individual account with different username and password.
2. Users must pass identity authentication before accessing the NAS. The authentication can be in local or centralized mode. It is recommended to combine the two modes, with centralized mode as active and local mode as standby. As a result, users must undergo authentication by the RADIUS server first. If the RADIUS server does not respond, it turns to local authentication.
3. During the authentication process, users can be classified and limited to access different NASs.
4. Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
5. The AAA records of users are stored on servers and can be viewed and referenced for auditing. (The TACACS+ server in this example performs the accounting.)

Figure 1-1



Remarks	User A, User B, and User C are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor. The TACACS+ server can be the dedicated server software provided by a vendor.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure the authentication service on the NAS.

- Configure the authorization service on the NAS.
- Configure the accounting service on the NAS.

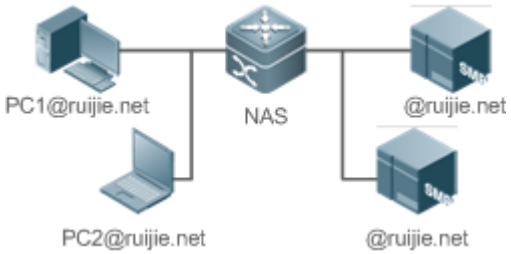
1.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@ruijie.net or PC2@ruijie.com.cn and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
- The AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 1-2



Remarks	The clients with the usernames **PC1@ruijie.net** and **PC2@ruijie.com.cn** are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The Security Accounts Manager (SAM) server is a universal RADIUS server.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Define an AAA method list on the NAS.
- Enable domain-based AAA on the NAS.
- Create domains and AV sets on the NAS.

1.3 Features

Basic Concepts

↘ **Local Authentication and Remote Server Authentication**

Local authentication is the process where the entered passwords are verified by the database on the NAS.

Remote server authentication is the process where the entered passwords are checked by the database on a remote server. It is mainly implemented by the RADIUS server and TACACS+ server.

Method List

AAA is implemented using different security methods. A method list defines a method implementation sequence. The method list can contain one or more security protocols so that a standby method can take over the AAA service when the first method fails. On devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a security method responds or all the security methods in the list are tried out. Authentication fails if no method in the list responds.

A method list contains a series of security methods that will be queried in sequence to verify user identities. It allows you to define one or more security protocols used for authentication, so that the standby authentication method takes over services when the active security method fails. On devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a method responds or all the methods in the method list are tried out. Authentication fails if no method in the list responds.

The next authentication method proceeds on devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 1-3

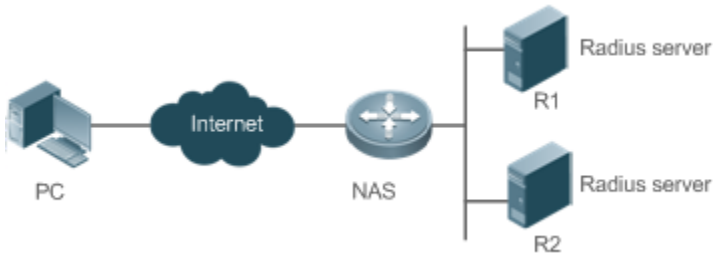


Figure 1-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

Assume that the system administrator defines a method list, where the NAS selects R1 and R2 in sequence to obtain user identity information and then accesses the local username database on the server. For example, when a remote PC user initiates dial-up access, the NAS first queries the user's identity on R1. When the authentication on R1 is completed, R1 returns an Accept response to the NAS. Then the user is permitted to access the Internet. If R1 returns a Reject response, the user is denied Internet access and the connection is terminated. If R1 does not respond, the NAS considers that the R1 method times out and continues to query the user's identity on R2. This process continues as the NAS keeps trying the remaining authentication methods, until the user request is authenticated, rejected, or terminated. If all the authentication methods are responded with Timeout, authentication fails and the connection will be terminated.

The Reject response is different from the Timeout response. The Reject response indicates that the user does not meet the criteria of the available authentication database and therefore fails in authentication, and the Internet access request is denied. The Timeout response indicates that the authentication server fails to respond to the identity query.

When detecting a timeout event, the AAA service proceeds to the next method in the list to continue the authentication process.

This document describes how to configure AAA on the RADIUS server. For details about the configuration on the TACACS+ server, see the *Configuring TACACS+*.

AAA Server Group

You can define an AAA server group to include one or more servers of the same type. If the server group is referenced by a method list, the NAS preferentially sends requests to the servers in the referenced server group when the method list is used to implement AAA.

Overview

Feature	Description
AAA Authentication	Verifies whether users can access the Internet.
AAA Authorization	Determines what services or permissions users can enjoy.
AAA Accounting	Records the network resource usage of users.
Multi-Domain AAA	Creates domain-specific AAA schemes for 802.1X stations (STAs) in different domains.

1.3.1 AAA Authentication

Authentication, authorization, and accounting are three independent services. The authentication service verifies whether users can access the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can use only the authentication service of AAA.

To configure AAA authentication, you need to first configure an authentication method list. Applications perform authentication according to the method list. The method list defines the types of authentication and the sequence in which they are performed. Authentication methods are implemented by specified applications. The only exception is the default method list. All applications use the default method list if no method list is configured.

AAA Authentication Scheme

- No authentication (**none**)

The identity of trusted users is not checked. Normally, the no-authentication (None) method is not used.

- Local authentication (**local**)

Authentication is performed on the NAS, which is configured with user information (including usernames, passwords, and AV pairs). Before local authentication is enabled, run the **username password/secret** command to create a local user database.

- Remote server group authentication (**group**)

Authentication is performed jointly by the NAS and a remote server group through RADIUS or TACACS+. A server group consists of one or more servers of the same type. User information is managed centrally on a remote server, thus realizing multi-device centralized and unified authentication with high capacity and reliability. You can configure local authentication as standby to avoid authentication failures when all the servers in the server group fail.

AAA Authentication Types

Products support the following authentication types:

- Login authentication

Users log in to the command line interface (CLI) of the NAS for authentication through Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).

- Enable authentication

After users log in to the CLI of the NAS, the users must be authenticated before CLI permission update. This process is called Enable authentication (in Privileged EXEC mode).

- Dot1X (IEEE802.1X) authentication

Dot1X (IEEE802.1X) authentication is performed for users that initiate dial-up access through IEEE802.1X.

- Web (second generation portal) authentication

Web authentication is performed by the second generation portal server.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Authentication Scheme

By default, no AAA authentication scheme is configured.

Before you configure an AAA authentication scheme, determine whether to use local authentication or remote server authentication. If the latter is to be implemented, configure a RADIUS or TACACS+ server in advance. If local authentication is selected, configure the local user database information on the NAS.

Configuring an AAA Authentication Method List

By default, no AAA authentication method list is configured.

Determine the access mode to be configured in advance. Then configure authentication methods according to the access mode.

1.3.2 AAA Authorization

AAA authorization allows administrators to control the services or permissions of users. After AAA authorization is enabled, the NAS configures the sessions of users according to the user configuration files stored on the NAS or servers. After authorization, users can use only the services or have only the permissions permitted by the configuration files.

AAA Authorization Scheme

- Direct authorization (**none**)

Direct authorization is intended for highly trusted users, who are assigned with the default permissions specified by the NAS.

- Local authorization (**local**)

Local authorization is performed on the NAS, which authorizes users according to the AV pairs configured for local users.

- Remote server-group authorization (**group**)

Authorization is performed jointly by the NAS and a remote server group. You can configure local or direct authorization as standby to avoid authorization failures when all the servers in the server group fail.

AAA Authorization Types

- EXEC authorization

After users log in to the CLI of the NAS, the users are assigned with permission levels (0 to 15).

- Config-commands authorization

Users are assigned with the permissions to run specific commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

After users log in through consoles, the users are authorized to run commands.

- Command authorization

Authorize users with commands after login to the CLI of the NAS.

- Network authorization

After users access the Internet, the users are authorized to use the specific session services. For example, after users access the Internet through PPP and Serial Line Internet Protocol (SLIP), the users are authorized to use the data service, bandwidth, and timeout service.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Authorization Scheme

By default, no AAA authorization scheme is configured.

Before you configure an AAA authorization scheme, determine whether to use local authorization or remote server-group authorization. If remote server-group authorization needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local authorization needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Authorization Method List

By default, no AAA authorization method list is configured.

Determine the access mode to be configured in advance. Then configure authorization methods according to the access mode.

1.3.3 AAA Accounting

In AAA, accounting is an independent process of the same level as authentication and authorization. During the accounting process, start-accounting, update-accounting, and end-accounting requests are sent to the configured accounting server, which records the network resource usage of users and performs accounting, audit, and tracking of users' activities.

In AAA configuration, accounting scheme configuration is optional.

AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

Accounting is completed on the NAS, which collects statistics on and limits the number of local user connections. Billing is not performed.

- Remote server-group accounting (**group**)

Accounting is performed jointly by the NAS and a remote server group. You can configure local accounting as standby to avoid accounting failures when all the servers in the server group fail.

AAA Accounting Types

- EXEC accounting

Accounting is performed when users log in to and out of the CLI of the NAS.

- Command accounting

Records are kept on the commands that users run on the CLI of the NAS.

- Network accounting

Records are kept on the sessions that users set up after completing 802.1X and Web authentication to access the Internet.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Accounting Scheme

By default, no AAA accounting method is configured.

Before you configure an AAA accounting scheme, determine whether to use local accounting or remote server-group accounting. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local accounting needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Accounting Method List

By default, no AAA accounting method list is configured.

Determine the access mode to be configured in advance. Then configure accounting methods according to the access mode.

1.3.4 Multi-Domain AAA

In a multi-domain environment, the NAS can provide the AAA services to users in different domains. The user AVs (such as usernames and passwords, service types, and permissions) may vary with different domains. It is necessary to configure domains to differentiate the user AVs in different domains and configure an AV set (including an AAA service method list, for example, RADIUS) for each domain.

Our products support the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

The fourth format (userid) does not contain a domain name, and it is considered to use the **default** domain name.

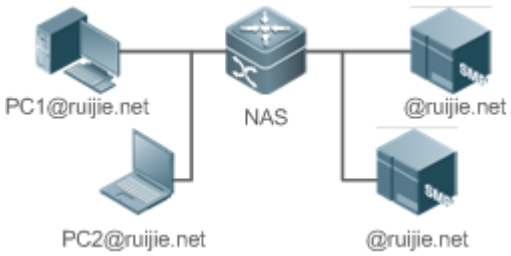
The NAS provides the domain-based AAA service based on the following principles:

- Resolves the domain name carried by a user.
- Searches for the user domain according to the domain name.
- Searches for the corresponding AAA method list name according to the domain configuration information on the NAS.
- Searches for the corresponding method list according to the method list name.
- Provides the AAA services based on the method list.

If any of the preceding procedures fails, the AAA services cannot be provided.

Figure 1-4 shows the typical multi-domain topology.

Figure 1-4



Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Method List

By default, no AAA method list is configured.

For details, see section 5.2.1, section 5.2.2, and section 5.2.3.

Enabling the Domain-Based AAA Service

By default, the domain-based AAA service is disabled.

To enable the domain-based AAA service, run the **aaa domain enable** command.

Creating a Domain

By default, no domain is configured.

To configure a domain, run the **aaa domain** *domain-name* command.

Configuring an AV Set for a Domain

By default, no domain AV set is configured.

A domain AV set contains the following elements: AAA method lists, the maximum number of online users, whether to remove the domain name from the username, and whether the domain name takes effect.

Displaying Domain Configuration

To display domain configuration, run the **show aaa domain** command.

The system supports a maximum of 32 domains.

1.4 Configuration

Configuration	Description and Command	
Configuring AAA Authentication	Mandatory if user identities need to be verified.	
	aaa new-model	Enables AAA.
	aaa authentication login	Defines a method list of login authentication.
	aaa authentication enable	Defines a method list of Enable authentication.
	aaa authentication dot1x	Defines a method list of 802.1X authentication.
	aaa authentication web-auth	Configures a method list of Web authentication.

Configuration	Description and Command	
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the maximum lockout time after a login failure.
Configuring AAA Authorization	Mandatory if different permissions and services need to be assigned to users.	
	aaa new-model	Enables AAA.
	aaa authorization exec	Defines a method list of EXEC authorization.
	aaa authorization commands	Defines a method list of command authorization.
	aaa authorization network	Configures a method list of network authorization.
	authorization exec	Applies EXEC authorization methods to a specified VTY line.
	authorization commands	Applies command authorization methods to a specified VTY line.
Configuring AAA Accounting	Mandatory if accounting, statistics, and tracking need to be performed on the network resource usage of users.	
	aaa new-model	Enables AAA.
	aaa accounting exec	Defines a method list of EXEC accounting.
	aaa accounting commands	Defines a method list of command accounting.
	aaa accounting network	Defines a method list of network accounting.
	accounting exec	Applies EXEC accounting methods to a specified VTY line.
	accounting commands	Applies command accounting methods to a specified VTY line.
	aaa accounting update	Enables accounting update.
	aaa accounting update periodic	Configures the accounting update interval.
Configuring an AAA Server Group	Recommended if a server group needs to be configured to handle AAA through different servers in the group.	
	aaa group server	Creates a user-defined AAA server group.
	server	Adds an AAA server group member.
Configuring the Domain-Based AAA Service	Mandatory if AAA management of 802.1X access STAs needs to be performed according to domains.	
	aaa new-model	Enables AAA.
	aaa domain enable	Enables the domain-based AAA service.

Configuration	Description and Command	
	aaa domain	Creates a domain and enters domain configuration mode.
	authentication dot1x	Associates the domain with an 802.1X authentication method list.
	accounting network	Associates the domain with a network accounting method list.
	authorization network	Associates the domain with a network authorization method list.
	state	Configures the domain status.
	username-format	Configures whether to contain the domain name in usernames.
	access-limit	Configures the maximum number of domain users.

1.4.1 Configuring AAA Authentication

Configuration Effect

Verify whether users are able to obtain access permission.

Notes

- If an authentication scheme contains multiple authentication methods, these methods are executed according to the configured sequence.
- The next authentication method is executed only when the current method does not respond. If the current method fails, the next method will be not tried.
- When the **none** method is used, users can get access even when no authentication method gets response. Therefore, the **none** method is used only as standby.

Normally, do not use None authentication. You can use the **none** method as the last optional authentication method in special cases. For example, all the users who may request access are trusted users and the users' work must not be delayed by system faults. Then you can use the **none** method to assign access permissions to these users when the authentication server does not respond. It is recommended that the local authentication method be added before the **none** method.

- If AAA authentication is enabled but no authentication method is configured and the default authentication method does not exist, users can directly log in to the Console without being authenticated. If users log in by other means, the users must pass local authentication.
- When a user enters the CLI after passing login authentication (the **none** method is not used), the username is recorded. When the user performs Enable authentication, the user is not prompted to enter the username again, because the username that the user entered during login authentication is automatically filled in. However, the user must enter the password previously used for login authentication.

- The username is not recorded if the user does not perform login authentication when entering the CLI or the **none** method is used during login authentication. Then, a user is required to enter the username each time when performing Enable authentication.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of Login Authentication

- Run the **aaa authentication login** command to configure a method list of login authentication.
- This configuration is mandatory if you need to configure a login authentication method list (including the configuration of the default method list).
- By default, no method list of login authentication is configured.

Defining a Method List of Enable Authentication

- Run the **aaa authentication enable** command to configure a method list of Enable authentication.
- This configuration is mandatory if you need to configure an Enable authentication method list. (You can configure only the default method list.)
- By default, no method list of Enable authentication is configured.

Defining a Method List of 802.1X Authentication

- Run the **aaa authentication dot1x** command to configure a method list of 802.1X authentication.
- This configuration is mandatory if you need to configure an 802.1X authentication method list (including the configuration of the default method list).
- By default, no method list of 802.1X authentication is configured.

Defining a Method List of Web Authentication

- Run the **aaa authentication web-auth** command to configure a method list of Web authentication.
- This configuration is mandatory if you need to configure a Web authentication method list (including the configuration of the default method list).
- By default, no method list of Web authentication is configured.

Setting the Maximum Number of Login Attempts

- Optional.
- By default, a user is allowed to enter passwords up to three times during login.

Setting the Maximum Lockout Time After a Login Failure

- Optional.
- By default, a user is locked for 15 minutes after entering wrong passwords three times.

Verification

- Run the **show aaa method-list** command to display the configured method lists.
- Run the **show aaa lockout** command to display the settings of the maximum number of login attempts and the maximum lockout time after a login failure.
- Run the **show running-config** command to display the authentication method lists associated with login authentication and 802.1X authentication.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of Login Authentication

Command	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default:** With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a login authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported. **subs**: Indicates that the subs database is used for authentication.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform login authentication negotiation through AAA. Run the **aaa authentication login** command to configure the default or optional method lists for login authentication. In a method list, the next method is executed only when the current method does not receive response. After you configure login authentication methods, apply the methods to the VTY lines that require login

	authentication; otherwise, the methods will not take effect.

Defining a Method List of Enable Authentication

Command	**aaa authentication enable default** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an Enable authentication method list in characters. *method*: Indicates authentication methods from **enable**, **local**, **none**, and **group**. A method list contains up to four methods. **enable**: Indicates that the password that is configured using the **enable** command is used for authentication. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform Enable authentication negotiation through AAA. Run the **aaa authentication enable** command to configure the default or optional method lists for Enable authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of 802.1X Authentication

Command	**aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an 802.1X authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server group is supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA 802.1X authentication service is enabled on the NAS, users must perform 802.1X authentication negotiation through AAA. Run the **aaa authentication dot1x** command to configure the default or optional method lists for 802.1X authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of Web Authentication

Command	**aaa authentication** { **web-auth** } { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**web-auth**: Configures a method list of Web authentication. **default**: With this parameter used, the configured method list will be defaulted.

	list-name: Indicates the name of a PPP authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported. **subs**: Specifies the SUBS authentication method using the SUBS database.
Command Mode	Global configuration mode
Usage Guide	If the AAA PPP authentication service is enabled on the NAS, users must perform PPP authentication negotiation through AAA. Run the **aaa authentication ppp** command to configure the default or optional method lists for PPP authentication. In a method list, the next method is executed only when the current method does not receive response.

Setting the Maximum Number of Login Attempts

Command	**aaa local authentication attempts** *max-attempts*
Parameter Description	*max-attempts*: Indicates the maximum number of login attempts. The value ranges from 1 to 2,147,483,647.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum number of times a user can attempt to login.

Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local authentication lockout-time** *lockout-time*
Parameter Description	*lockout-time*: Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 2,147,483,647, in the unit of minutes.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum time during which a user is locked after entering wrong passwords up to the specified times.

Configuration Example

Configuring AAA Login Authentication

Configure a login authentication method list on the NAS containing **group** *radius* and **local** methods in order.

Scenario Figure 1-5	

Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Step 3: Configure an AAA authentication method list for login authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication login list1 group radius local Hostname(config)#line vty 0 20 Hostname(config-line)#login authentication list1 Hostname(config-line)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login list1 group radius local Accounting method-list: Authorization method-list:
	Assume that a user remotely logs in to the NAS through Telnet. The user is prompted to enter the username and password on the CLI. The user must enter the correct username and password to access the NAS.
User	User Access Verification Username:user Password:pass

Configuring AAA Enable Authentication

Configure an Enable authentication method list on the NAS containing **group** *radius*, **local**, and then **enable** methods in order.

Scenario **Figure 1-6**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication. Step 3: Configure an AAA authentication method list for Enable authentication users. You can define only one Enable authentication method list globally. You do not need to define the list name but just default it. After that, it will be applied automatically.

NAS	`Hostname#configure terminal`
	`Hostname(config)#username user privilege 15 password pass`
	`Hostname(config)#enable secret w`
	`Hostname(config)#aaa new-model`
	`Hostname(config)#radius-server host 10.1.1.1`
	`Hostname(config)#radius-server key test`
	`Hostname(config)#aaa authentication enable default group radius local enable`

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

NAS	`Hostname#show aaa method-list`
	
	`Authentication method-list:`
	`aaa authentication enable default group radius local enable`
	
	`Accounting method-list:`
	
	`Authorization method-list:`

	The CLI displays an authentication prompt when the user level is updated to level 15. The user must enter the correct username and password to access the NAS.
NAS	Hostname>enable Username:user Password:pass Hostname#

Configuring AAA 802.1X Authentication

Configure an 802.1X authentication method list on the NAS containing **group** *radius*, and then **local** methods in order.

Scenario **Figure 1-7**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Currently, 802.1X authentication does not support TACACS+. Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the AAA authentication method list. Skip this step if the default authentication method is used. Step 5: Enable 802.1X authentication on an interface.
NAS	Hostname#configure terminal Hostname(config)#username user1 password pass1 Hostname(config)#username user2 password pass2 Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication dot1x default group radius local Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)#dot1 port-control auto Hostname(config-if-gigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.

NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication dot1x default group radius local Accounting method-list: Authorization method-list:

Common Errors

- No RADIUS server or TACACS+ server is configured.
- Usernames and passwords are not configured in the local database.

1.4.2 Configuring AAA Authorization

Configuration Effect

- Determine what services or permissions authenticated users can enjoy.

Notes

- EXEC authorization is often used with login authentication, which can be implemented on the same line. Authorization and authentication can be performed using different methods and servers. Therefore, the results of the same user may be different. If a user passes login authentication but fails in EXEC authorization, the user cannot enter the CLI.
- The authorization methods in an authorization scheme are executed in accordance with the method configuration sequence. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried.
- Command authorization is supported only by TACACS+.
- Console authorization: System can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Steps

↘ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Authorization

- Run the **aaa authorization exec** command to configure a method list of EXEC authorization.
- This configuration is mandatory if you need to configure an EXEC authorization method list (including the configuration of the default method list).
- By default, no EXEC authorization method list is configured.

The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)

Defining a Method List of Command Authorization

- Run the **aaa authorization commands** command to configure a method list of command authorization.
- This configuration is mandatory if you need to configure a command authorization method list (including the configuration of the default method list).
- By default, no command authorization method list is configured.

Configuring a Method List of Network Authorization

- Run the **aaa authorization network** command to configure a method list of network authorization.
- This configuration is mandatory if you need to configure a network authorization method list (including the configuration of the default method list).
- By default, no authorization method is configured.

Applying EXEC Authorization Methods to a Specified VTY Line

- Run the **authorization exec** command in line configuration mode to apply EXEC authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Applying Command Authorization Methods to a Specified VTY Line

- Run the **authorization commands** command in line configuration mode to apply command authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Enabling Authorization for Commands in Configuration Modes

- Run the **aaa authorization config-commands** command to enable authorization for commands in configuration modes.
- By default, authorization is disabled for commands in configuration modes.

Enabling Authorization for the Console to Run Commands

- Run the **aaa authorization console** command to enable authorization for console users to run commands.
- By default, authorization is disabled for the Console to run commands.

Verification

Run the **show running-config** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Authorization

Command	**aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC authorization method list in characters. *method*: Specifies authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for EXEC authorization. **none**: Indicates that EXEC authorization is not performed. **group**: Indicates that a server group is used for EXEC authorization. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	System supports authorization of the users who log in to the CLI of the NAS to assign the users CLI operation permission levels (0 to 15). Currently, EXEC authorization is performed only on the users who have passed login authentication. If a user fails in EXEC authorization, the user cannot enter the CLI. After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.

Defining a Method List of Command Authorization

Command	**aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command authorization is not performed.

	group: Indicates that a server group is used for command authorization. Currently, the TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	System supports authorization of the commands executable by users. When a user enters a command, AAA sends the command to the authentication server. If the authentication server permits the execution, the command is executed. If the authentication server forbids the execution, the command is not executed and a message is displayed showing that the execution is rejected. When you configure command authorization, specify the command level, which is used as the default level. (For example, if a command above Level 14 is visible to users, the default level of the command is 14.) After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.

Configuring a Method List of Network Authorization

Command	**aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for network authorization. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	System supports authorization of network-related service requests such as PPP and SLIP requests. After authorization is configured, all authenticated users or interfaces are authorized automatically. You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried. RADIUS or TACACS+ servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.

Enabling Authorization for Commands in Configuration Modes (Including the Global Configuration Mode and Sub-Modes)

Command	**aaa authorization config-commands**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If you need to enable authorization for commands only in non-configuration modes (for example, privileged EXEC mode), disable authorization in configuration modes by using the **no** form of this command. Then

	users can run commands in configuration mode and sub-modes without authorization.

Enabling Authorization for the Console to Run Commands

Command	**aaa authorization console**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	System can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Example

Configuring AAA EXEC Authorization

Configure login authentication and EXEC authorization for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC authorization is performed on a RADIUS server. If the RADIUS server does not respond, users are redirected to the local authorization.

Scenario Figure 1-8	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used. EXEC authorization is often used with login authentication, which can be implemented on the same line.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#username user privilege 6 Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication login list1 group local

	Hostname(config)#aaa authorization exec list2 group radius local Hostname(config)#line vty 0 4 Hostname(config-line)#login authentication list1 Hostname(config-line)# authorization exec list2 Hostname(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to displaythe configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: Authorization method-list: aaa authorization exec list2 group radius local
	Hostname# show running-config aaa new-model ! aaa authorization exec list2 group local aaa authentication login list1 group radius local ! username user password pass username user privilege 6 ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 authorization exec list2

	login authentication list1 ! End

Configuring AAA Command Authorization

Provide command authorization for login users according to the following default authorization method: Authorize level-15 commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is performed. Authorization is applied to the users who log in through the Console and the users who log in through other types of clients.

Scenario **Figure 1-9**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	Hostname#configure terminal Hostname(config)#username user1 password pass1 Hostname(config)#username user1 privilege 15 Hostname(config)#aaa new-model Hostname(config)#tacacs-server host 192.168.217.10 Hostname(config)#tacacs-server key aaa Hostname(config)#aaa authentication login default local Hostname(config)#aaa authorization commands 15 default group tacacs+ local Hostname(config)#aaa authorization console
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login default local

	Accounting method-list: Authorization method-list: aaa authorization commands 15 default group tacacs+ local
	Hostname#show run ! aaa new-model ! aaa authorization console aaa authorization commands 15 default group tacacs+ local aaa authentication login default local ! ! nfpp ! vlan 1 ! username user1 password 0 pass1 username user1 privilege 15 no service password-encryption ! tacacs-server host 192.168.217.10 tacacs-server key aaa ! line con 0 line vty 0 4 ! ! end

Configuring AAA Network Authorization

Scenario **Figure 1-10**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	Hostname#configure terminal Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authorization network default group radius none Hostname(config)# end
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none

Common Errors

N/A

1.4.3 Configuring AAA Accounting

Configuration Effect

- Record the network resource usage of users.

- Record the user login and logout processes and the commands executed by users during device management.

Notes

About accounting methods:

- If an accounting scheme contains multiple accounting methods, these methods are executed according to the method configuration sequence. The next accounting method is executed only when the current method does not receive response. If accounting fails using a method, the next method will be not tried.
- After the default accounting method list is configured, it is applied to all VTY lines automatically. If a non-default accounting method list is applied to a line, it will replace the default one. If you apply an undefined method list to a line, the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

- EXEC accounting is performed only when login authentication on the NAS is completed. EXEC accounting is not performed if login authentication is not configured or the **none** method is used for authentication. If Start accounting is not performed for a user upon login, Stop accounting will not be performed when the user logs out.

Command accounting

- Only the TACACS+ protocol supports command accounting.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Accounting

- Run the **aaa accounting exec** command to configure a method list of EXEC accounting.
- This configuration is mandatory if you need to configure an EXEC accounting method list (including the configuration of the default method list).
- The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)
- By default, no EXEC accounting method list is configured.

Defining a Method List of Command Accounting

- Run the **aaa accounting commands** command to configure a method list of command accounting.
- This configuration is mandatory if you need to configure a command accounting method list (including the configuration of the default method list).

- By default, no command accounting method list is configured. Only the TACACS+ protocol supports command accounting.

Defining a Method List of Network Accounting

- Run the **aaa accounting network** command to configure a method list of network accounting.
- This configuration is mandatory if you need to configure a network accounting method list (including the configuration of the default method list).
- By default, no network accounting method list is configured.

Applying EXEC Accounting Methods to a Specified VTY Line

- Run the **accounting exec** command in line configuration mode to apply EXEC accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying Command Accounting Methods to a Specified VTY Line

- Run the **accounting commands** command in line configuration mode to apply command accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying 802.1X Network Accounting Methods

- Run the **dot1x accounting network** command to configure 802.1X network accounting methods.
- This configuration is mandatory if you need to specify 802.1X network accounting methods.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Enabling Accounting Update

- Optional.
- It is recommended that accounting update be configured for improved accounting accuracy.
- By default, accounting update is disabled.

Configuring the Accounting Update Interval

- Optional.
- It is recommended that the accounting update interval not be configured unless otherwise specified.

Verification

Run the **show running-config** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Accounting

Command	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that EXEC accounting is not performed. **group**: Indicates that a server group is used for EXEC accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	System enables EXEC accounting only when login authentication is completed. EXEC accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, when a user logs in to the CLI of the NAS, the NAS sends a start-accounting message to the authentication server. When the user logs out, the NAS sends a stop-accounting message to the authentication server. If the NAS does not send a start-accounting message when the user logs in, the NAS will not send a stop-accounting message when the user logs out. After you configure EXEC accounting methods, apply the methods to the VTY lines that require EXEC accounting; otherwise, the methods will not take effect.

Defining a Method List of Command Accounting

Command	**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*level*: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15. After a command of the configured level is executed, the accounting server records related information based on the received accounting packet. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods.

	none: Indicates that command accounting is not performed. **group**: Indicates that a server group is used for command accounting. Currently, the TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	System enables command accounting only when login authentication is completed. Command accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, the NAS records information about the commands of the configured level that users run and sends the information to the authentication server. After you configure command accounting methods, apply the methods to the VTY lines that require command accounting; otherwise, the methods will not take effect.

Defining a Method List of Network Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network accounting method list in characters. **start-stop**: Indicates that a start-accounting message and a stop-accounting message are sent when a user accesses a network and when the user disconnects from the network respectively. The start-accounting message indicates that the user is allowed to access the network, regardless of whether accounting is successfully enabled. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that network accounting is not performed. **group**: Indicates that a server group is used for network accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	System sends record attributes to the authentication server to perform accounting of user activities. The **start-stop** keyword is used to configure user accounting options.

Enabling Accounting Update

Command	**aaa accounting update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to enable accounting update.

Configuring the Accounting Update Interval

Command	**aaa accounting update periodic** *interval*
Parameter	*Interval*: Indicates the accounting update interval, in the unit of minutes. The shortest is 1 minute.

Description	
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to configure the accounting update interval.

Configuration Example

↘ Configuring AAA EXEC Accounting

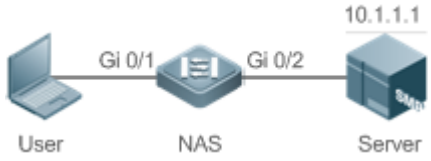
Configure login authentication and EXEC accounting for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC accounting is performed on a RADIUS server.

Scenario Figure 1-11	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication login list1 group local Hostname(config)#aaa accounting exec list3 start-stop group radius Hostname(config)#line vty 0 4 Hostname(config-line)#login authentication list1 Hostname(config-line)# accounting exec list3 Hostname(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to displaythe configuration.
NAS	Hostname#show aaa method-list

	Authentication method-list: aaa authentication login list1 group local Accounting method-list: aaa accounting exec list3 start-stop group radius Authorization method-list:
	Hostname# show running-config aaa new-model ! aaa accounting exec list3 start-stop group radius aaa authentication login list1 group local ! username user password pass ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 accounting exec list3 login authentication list1 ! End

Configuring AAA Command Accounting

Configure command accounting for login users according to the default accounting method. Login authentication is performed in local mode, and command accounting is performed on a TACACS+ server.

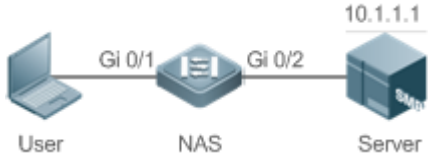
Scenario **Figure 1-12**	

Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	Hostname#configure terminal Hostname(config)#username user1 password pass1 Hostname(config)#username user1 privilege 15 Hostname(config)#aaa new-model Hostname(config)#tacacs-server host 192.168.217.10 Hostname(config)#tacacs-server key aaa Hostname(config)#aaa authentication login default local Hostname(config)#aaa accounting commands 15 default start-stop group tacacs+
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: aaa accounting commands 15 default start-stop group tacacs+ Authorization method-list:
	Hostname#show run ! aaa new-model ! aaa authorization config-commands aaa accounting commands 15 default start-stop group tacacs+ aaa authentication login default local

```
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

Configuring AAA Network Accounting

Configure a network accounting method list for 802.1X STAs, and configure a RADIUS remote server for authentication and accounting.

Scenario Figure 1-13	
Configuration Steps	Step 1: Enable AAA. Step 2: If remote server-group accounting needs to be implemented, configure a RADIUS server in advance. Step 3: Configure an AAA accounting method list according to different access modes and service types. Step 4: Apply the configured AAA accounting method list. Skip this step if the default accounting method is used. Accounting is performed only when 802.1X authentication is completed.

NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication dot1x aut1x group radius local Hostname(config)#aaa accounting network acc1x start-stop group radius Hostname(config)#dot1x authentication aut1x Hostname(config)#dot1x accounting acc1x Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#dot1 port-control auto Hostname(config-if-GigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to displaythe configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication dot1x aut1x group radius local Accounting method-list: aaa accounting network acc1x start-stop group radius Authorization method-list:

Common Errors

N/A

1.4.4 Configuring an AAA Server Group

Configuration Effect

- Create a user-defined server group and add one or more servers to the group.
- When you configure authentication, authorization, and accounting method lists, name the methods after the server group name so that the servers in the group are used to handle authentication, authorization, and accounting requests.
- Use self-defined server groups to separate authentication, authorization, and accounting.

Notes

In a user-defined server group, you can specify and apply only the servers in the default server group.

Configuration Steps

Creating a User-Defined AAA Server Group

- Mandatory.
- Assign a meaningful name to the user-defined server group. Do not use the predefined **radius** and **tacacs+** keywords in naming.

Adding an AAA Server Group Member

- Mandatory.
- Run the **server** command to add AAA server group members.
- By default, a user-defined server group does not have servers.

Verification

Run the **show aaa group** command to verify the configuration.

Related Commands

Creating a User-Defined AAA Server Group

Command	**aaa group server** {**radius** | **tacacs+**} *name*
Parameter Description	*name*: Indicates the name of the server group to be created. The name must not contain the **radius** and **tacacs+** keywords because they are the names of the default RADIUS and TACACS+ server groups.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.

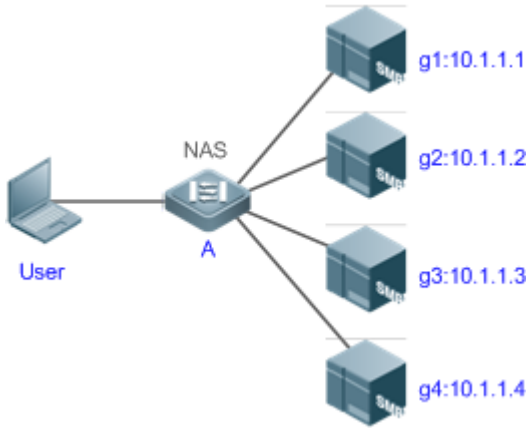
Adding an AAA Server Group Member

Command	**server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-addr*: Indicates the IP address of a server. *port1*: Indicates the authentication port of a server. (This parameter is supported only by the RADIUS server group.) *port2*: Indicates the accounting port of a server. (This parameter is supported only by the RADIUS server group.)
Command Mode	Server group configuration mode
Usage Guide	When you add servers to a server group, the default ports are used if you do not specify ports.

Configuration Example

Creating an AAA Server Group

Create RADIUS server groups named g1 and g2. The IP addresses of the servers in g1 are 10.1.1.1 and 10.1.1.2, and the IP addresses of the servers in g2 are 10.1.1.3 and 10.1.1.4.

Scenario **Figure 1-14**	
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable. 2. Enable AAA.
Configuration Steps	Step 1: Configure a server (which belongs to the default server group). Step 2: Create user-defined AAA server groups. Step 3: Add servers to the AAA server groups.
NAS	Hostname#configure terminal Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server host 10.1.1.2 Hostname(config)#radius-server host 10.1.1.3 Hostname(config)#radius-server host 10.1.1.4 Hostname(config)#radius-server key secret Hostname(config)#aaa group server radius g1 Hostname(config-gs-radius)#server 10.1.1.1 Hostname(config-gs-radius)#server 10.1.1.2 Hostname(config-gs-radius)#exit Hostname(config)#aaa group server radius g2 Hostname(config-gs-radius)#server 10.1.1.3 Hostname(config-gs-radius)#server 10.1.1.4 Hostname(config-gs-radius)#exit

Verification	Run the **show aaa group** and **show run** commands on the NAS to display the configuration.
NAS	Hostname#show aaa group Type Reference Name ---------- ---------- ---------- radius 1 radius tacacs+ 1 tacacs+ radius 1 g1 radius 1 g2
	Hostname#show run ! 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 secret ! aaa group server radius g1 server 10.1.1.1 server 10.1.1.2 ! aaa group server radius g2 server 10.1.1.3 server 10.1.1.4 ! !

Common Errors

- For RADIUS servers that use non-default authentication and accounting ports, when you run the **server** command to add servers, specify the authentication or accounting port.

1.4.5 Configuring the Domain-Based AAA Service

Configuration Effect

Create AAA schemes for 802.1X users in different domains.

Notes

About referencing method lists in domains:

- The AAA method lists that you select in domain configuration mode should be defined in advance. If the method lists are not defined in advance, when you select them in domain configuration mode, the system prompts that the configurations do not exist.
- The names of the AAA method lists selected in domain configuration mode must be consistent with those of the method lists defined for the AAA service. If they are inconsistent, the AAA service cannot be properly provided to the users in the domain.

About the default domain:

- Default domain: After the domain-based AAA service is enabled, if a username does not carry domain information, the AAA service is provided to the user based on the default domain. If the domain information carried by the username is not configured in the system, the system determines that the user is unauthorized and will not provide the AAA service to the user. If the default domain is not configured initially, it must be created manually.
- When the domain-based AAA service is enabled, the default domain is not configured by default and needs to be created manually. The default domain name is **default**. It is used to provide the AAA service to the users whose usernames do not carry domain information. If the default domain is not configured, the AAA service is not available for the users whose usernames do not carry domain information.

About domain names:

- The domain names carried by usernames and those configured on the NAS are matched in the longest matching principle. For example, if two domains, **domain.com** and **domain.com.cn** are configured on a NAS and a user sends a request carrying **aaa@domain.com**, the NAS determines that the user belongs to **domain.com**, instead of **domain.com.cn**.
- If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the AAA service is not provided to the user.

Configuration Steps

↘ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

↘ Enabling the Domain-Based AAA Service

- Mandatory.
- Run the **aaa domain enable** command to enable the domain-based AAA service.
- By default, the domain-based AAA service is disabled.

Creating a Domain and Entering Domain Configuration Mode

- Mandatory.
- Run the **aaa domain** command to create a domain or enter the configured domain.
- By default, no domain is configured.

Associating the Domain with an 802.1X Authentication Method List

- Run the **authentication dot1x** command to associate the domain with an 802.1X authentication method list.
- This configuration is mandatory if you need to apply a specified 802.1X authentication method list to the domain.
- Currently, the domain-based AAA service is applicable only to 802.1X access.

Associating the Domain with a Network Accounting Method List

- Run the **accounting network** command to associate the domain with a network accounting method.
- This configuration is mandatory if you need to apply a specified network accounting method list to the domain.
- If a domain is not associated with a network accounting method list, by default, the global default method list is used for accounting.

Associating the Domain with a Network Authorization Method List

- Run the **authorization network** command to associate the domain with a network authorization method list.
- This configuration is mandatory if you need to apply a specified network authorization method list to the domain.
- If a domain is not associated with a network authorization method list, by default, the global default method list is used for authorization.

Configuring the Domain Status

- Optional.
- When a domain is in Block state, the users in the domain cannot log in.
- By default, after a domain is created, its state is Active, indicating that all the users in the domain are allowed to request network services.

Configuring Whether to Contain the Domain Name in Usernames

- Optional.
- By default, the usernames exchanged between the NAS and an authentication server carry domain information.

Configuring the Maximum Number of Domain Users

- Optional.
- By default, the maximum number of access users allowed in a domain is not limited.

Verification

Run the **show aaa domain** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Enabling the Domain-Based AAA Service

Command	**aaa domain enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the domain-based AAA service.

Creating a Domain and Entering Domain Configuration Mode

Command	**aaa domain** { **default** | *domain-name* }
Parameter Description	**default**: Uses this parameter to configure the default domain. *domain-name*: Indicates the name of the domain to be created.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a domain to provide the domain-based AAA service. The **default** parameter specifies the default domain. If a username does not carry domain information, the NAS uses the method list associated with the default domain to provide the AAA service to the user. The *domain-name* parameter specifies the name of the domain to be created. If the domain name carried by a username matches the configured domain name, the NAS uses the method list associated with this domain to provide the AAA service to the user. The system supports a maximum of 32 domains.

Associating the Domain with an 802.1X Authentication Method List

Command	**authentication dot1x** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a 802.1X authentication method list.

Associating the Domain with a Web Authentication Method List

Command	**authentication web-auth** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a Web authentication method list.

Associating the Domain with a Network Accounting Method List

Command	**accounting network** { **default |** *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a network accounting method list.

Associating the Domain with a Network Authorization Method List

Command	**authorization network** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	

Configuring the Domain Status

Command	**state** { **block** | **active** }
Parameter Description	**block**: Indicates that the configured domain is invalid. **active**: Indicates that the configured domain is valid.
Command Mode	Domain configuration mode
Usage Guide	Use this command to make the configured domain valid or invalid.

Configuring Whether to Contain the Domain Name in Usernames

Command	**username-format** { **without-domain** | **with-domain** }
Parameter Description	**without-domain**: Indicates to remove domain information from usernames. **with-domain**: Indicates to keep domain information in usernames.
Command Mode	Domain configuration mode
Usage Guide	Use this command in domain configuration mode to determine whether to include domain information in

	usernames when the NAS interacts with authentication servers in a specified domain.

Configuring the Maximum Number of Domain Users

Command	**access-limit** *num*
Parameter Description	*num*: Indicates the maximum number of access users allowed in a domain. This limit is applicable only to 802.1X STAs.
Command Mode	Domain configuration mode
Usage Guide	Use this command to limit the number of access users in a domain.

Configuration Example

Configuring the Domain-Based AAA Services

Configure authentication and accounting through a RADIUS server to 802.1X users (username: *user*@domain.com) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain information, and the number of access users is not limited.

Scenario Figure 1-15	
Configuration Steps	The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance. Step 1: Enable AAA. Step 2: Define an AAA method list. Step 3: Enable the domain-based AAA service. Step 4: Create a domain. Step 5: Associate the domain with the AAA method list. Step 6: Configure the domain attribute.
NAS	Hostname#configure terminal Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication dot1x default group radius Hostname(config)#aaa accounting network list3 start-stop group radius Hostname(config)# aaa domain enable Hostname(config)# aaa domain domain.com Hostname(config-aaa-domain)# authentication dot1x default

	Hostname(config-aaa-domain)# accounting network list3 Hostname(config-aaa-domain)# username-format without-domain
Verification	Run the **show run** and **show aaa domain** command on the NAS to displaythe configuration.
NAS	Hostname#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
	Hostname#show run Building configuration... Current configuration : 1449 bytes version system 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67) co-operate enable ! aaa new-model aaa domain enable ! aaa domain domain.com authentication dot1x default accounting network list3 ! aaa accounting network list3 start-stop group radius aaa authentication dot1x default group radius

```
!
nfpp
!
no service password-encryption
!
radius-server host 10.1.1.1
radius-server key test
!
line con 0
line vty 0 4
!
end
```

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the locked users.	**clear aaa local user lockout** {**all** | **user-name** *username* }

Displaying

Description	Command
Displays the accounting update information.	**show aaa accounting update**
Displays the current domain configuration.	**show aaa domain**
Displays the current lockout configuration.	**show aaa lockout**
Displays the AAA server groups.	**show aaa group**
Displays the AAA method lists.	**show aaa method-list**
Displays the AAA users.	**show aaa user**

2 Configuring RADIUS

2.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system.

RADIUS works with the Authentication, Authorization, and Accounting (AAA) to conduct identity authentication on users who attempt to access a network, to prevent unauthorized access. In system implementation, a RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the central RADIOUS server, where all user identity authentication information and network service information are stored. In addition to the authentication service, the RADIUS server provides authorization and accounting services for access users.

RADIUS is often applied in network environments that have high security requirements and allow the access of remote users. RADIUS is a completely open protocol and the RADIUS server is installed on many operating systems as a component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server currently.

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service is defined in the IETF RFC3576. This protocol defines a user offline management method. Devices communicate with the RADIUS server through the Disconnect-Messages (DMs) to bring authenticated users offline. This protocol implements compatibility between devices of different vendors and the RADIUS server in terms of user offline processing.

In the DM mechanism, the RADIUS server actively initiates a user offline request to a device, the device locates a user according to the user session information, user name, and other information carried in the request and brings the user offline. Then, the device returns a response packet that carries the processing result to the RADIUS server, thereby implementing user offline management of the RADIUS server.

Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

2.2 Applications

Application	Description
Providing Authentication, Authorization, and Accounting	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.

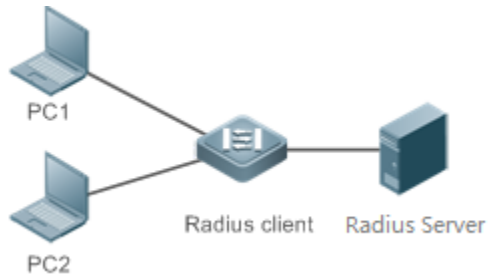
Application	Description
Services for Access Users	
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

2.2.1 Providing Authentication, Authorization, and Accounting Services for Access Users

Scenario

RADIUS is typically applied in the authentication, authorization, and accounting of access users. A network device serves as a RADIUS client and transmits user information to a RADIUS server. After completing processing, the RADIUS server returns the authentication acceptance/authentication rejection/accounting response information to the RADIUS client. The RADIUS client performs processing on the access user according to the response from the RADIUS server.

Figure 2-1 Typical RADIUS Networking Topology



Remarks	PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, and initiate authentication and accounting requests. The RADIUS client is usually an access switch or aggregate switch. The RADIUS server can be a component built in the Windows 2000/2003, Server (IAS), or UNIX operating system or dedicated server software provided by vendors.

Deployment

- Configure access device information on the RADIUS server, including the IP address and shared key of the access devices.
- Configure the AAA method list on the RADIUS client.
- Configure the RADIUS server information on the RADIUS client, including the IP address and shared key.
- Enable access control on the access port of the RADIUS client.
- Configure the network so that the RADIUS client communicates with the RADIUS server successfully.

2.2.2 Forcing Users to Go Offline

Scenario

The RADIUS server forces authenticated online users to go offline for the sake of management.

See Figure 2-1 for the networking topology.

Deployment

- Add the following deployment on the basis of 1.2.1 "Deployment".
- Enable the RADIUS dynamic authorization extension function on the RADIUS client.

2.3 Features

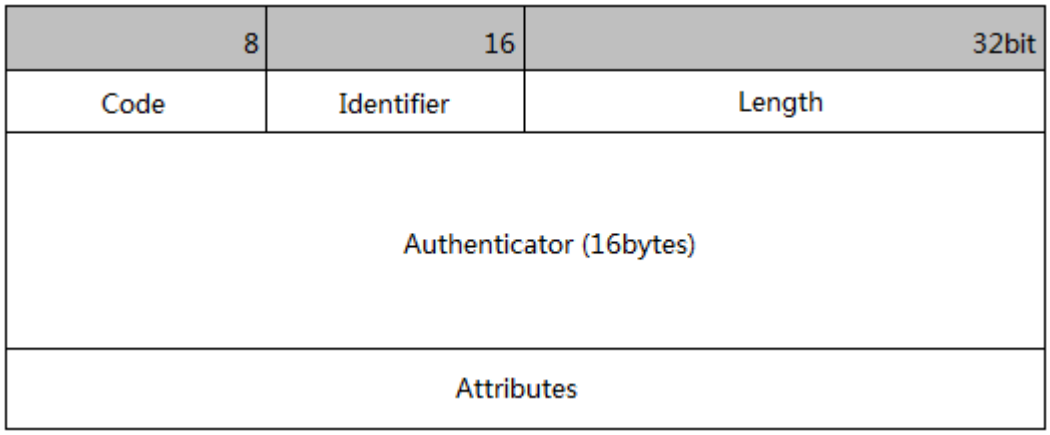
Basic Concepts

Client/Server Mode

- Client: A RADIUS client initiates RADIUS requests and usually runs on a device or NAS. It transmits user information to the RADIUS server, receives responses from the RADIUS server, and performs processing accordingly. The processing includes accepting user access, rejecting user access, or collecting more user information for the RADIUS server.
- Server: Multiple RADIUS clients map to one RADIUS server. The RADIUS server maintains the IP addresses and shared keys of all RADIUS clients as well as information on all authenticated users. It receives requests from a RADIUS client, conducts authentication, authorization, and accounting, and returns processing information to the RADIUS client.

Structure of RADIUS Packets

The following figure shows the structure of RADIUS packets.



- Code: Identifies the type of RADIUS packets, which occupies one byte. The following table lists the values and meanings.

Code	Packet Type	Code	Packet Type
1	Access-Request	4	Accounting-Request
2	Access-Accept	5	Accounting-Response
3	Access-Reject	11	Access-Challenge

- Identifier: Indicates the identifier for matching request packets and response packets, which occupies one byte. The identifier values of request packets and response packets of the same type are the same.

- Length: Identifies the length of a whole RADIUS packet, which includes **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes**. It occupies two bytes. Bytes that are beyond the **Length** field will be truncated. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.
- Authenticator: Verifies response packets of the RADIUS server by a RADIUS client, which occupies 16 bytes. This field is also used for encryption/decryption of user passwords.
- Attributes: Carries authentication, authorization, and accounting information, with the length unfixed. The **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type, Length, Value (TLV) format. Type occupies one byte and indicates the attribute type. The following table lists common attributes of RADIUS authentication, authorization, and accounting. Length occupies one byte and indicates the attribute length, with the unit of bytes. Value indicates the attribute information.

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
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

Attribute No.	Attribute Name	Attribute No.	Attribute Name
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

Shared Key

A RADIUS client and a RADIUS server mutually confirm their identities by using a shared key during communication. The shared key cannot be transmitted over a network. In addition, user passwords are encrypted for transmission for the sake of security.

RADIUS Server Group

The RADIUS security protocol, also called RADIUS method, is configured in the form of a RADIUS server group. Each RADIUS method corresponds to one RADIUS server group and one or more RADIUS severs can be added to one RADIUS server group. For details about the RADIUS method, see the *Configuring AAA*. If you add multiple RADIUS servers to one RADIUS server group, when the communication between a device and the first RADIUS server in this group fails or the first RADIUS server becomes unreachable, the device automatically attempts to communicate with the next RADIUS server till the communication is successful or the communication with all the RADIUS servers fails.

RADIUS Attribute Type

- Standard attributes

The RFC standards specify the RADIUS attribute numbers and attribute content but do not specify the format of some attribute types. Therefore, the format of attribute contents needs to be configured to adapt to different RADIUS server requirements. Currently, the format of the RADIUS Calling-Station-ID attribute (attribute No.: 31) can be configured.

The RADIUS Calling-Station-ID attribute is used to identify user identities when a network device transmits request packets to the RADIUS server. The RADIUS Calling-Station-ID attribute is a string, which can adopt multiple formats. It needs to uniquely identify a user. Therefore, it is often set to the MAC address of a user. For example, when IEEE 802.1X authentication is used, the Calling-Station-ID attribute is set to the MAC address of the device where the IEEE 802.1X client is installed. The following table describes the format of MAC addresses.

Format	Description
Ietf	Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC
Normal	Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac
Unformatted	Indicates the format without separators. This format is used by default. Example: 00d0f83322ac

- Private attributes

RADIUS is an extensible protocol. According to RFC2865, the Vendor-Specific attribute (attribute No.: 26) is used by device vendors to extend the RADIUS protocol to implement private functions or functions that are not defined in the standard RADIUS protocol. Table 1-3 lists private attributes supported by Hostname products. The **TYPE** column indicates the default configuration of private attributes of Hostname products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-Hostname products.

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
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42

ID	Function	TYPE	Extended TYPE
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

Overview

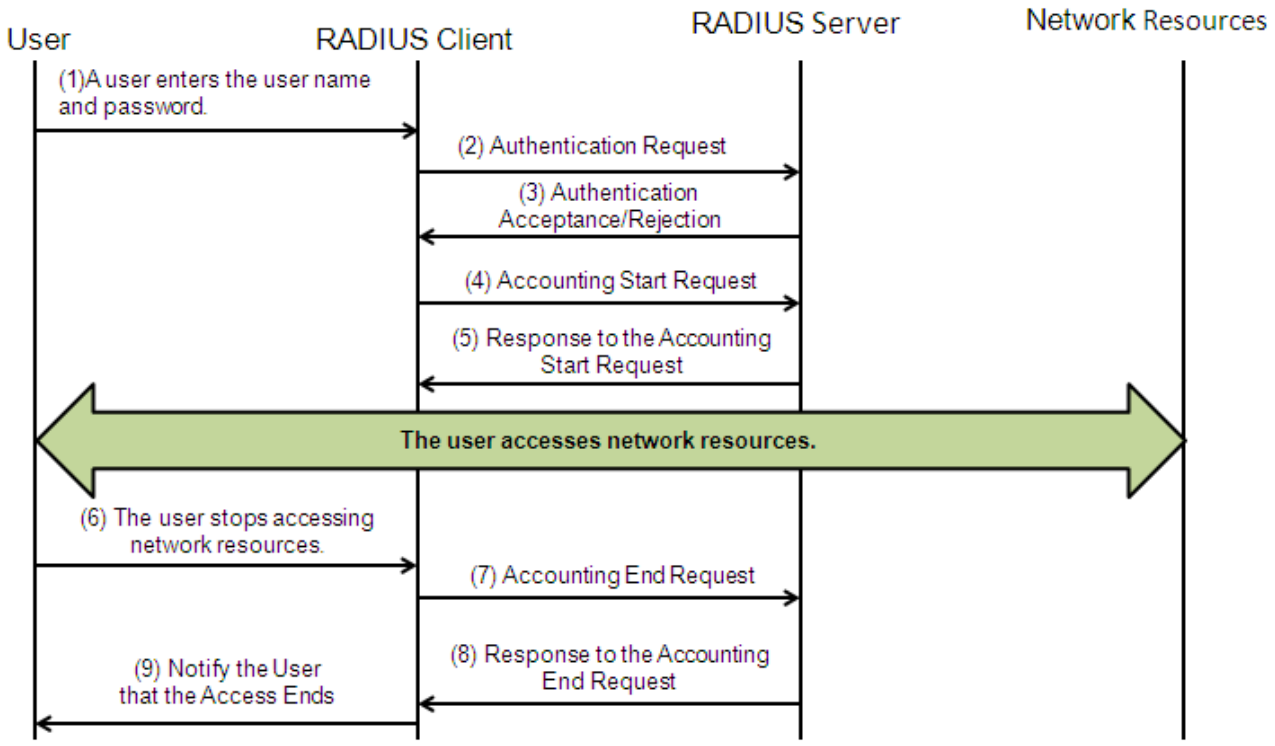
Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.
RADIUS Timeout Retransmission	Specifies the packet retransmission parameter for a RADIUS client when a RADIUS server does not respond to packets transmitted from the RADIUS client within a period of time.
RADIUS Server Accessibility Detection	Enables a RADIUS client to actively detect whether a RADIUS server is reachable and maintain the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.
RADIUS Forced Offline	Enables a RADIUS server to actively force authenticated users to go offline.

2.3.1 RADIUS Authentication, Authorization, and Accounting

Conduct identity authentication and accounting on access users, safeguard network security, and facilitate management for network administrators.

Working Principle

Figure 2-2



The RADIUS authentication and authorization process is described as follows:

1. A user enters the user name and password and transmits them to the RADIUS client.
2. After receiving the user name and password, the RADIUS client transmits an authentication request packet to the RADIUS server. The password is encrypted for transmission. For the encryption method, see RFC2865.
3. The RADIUS server accepts or rejects the authentication request according to the user name and password. When accepting the authentication request, the RADIUS server also issues authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.
4. The RADIUS accounting process is described as follows:
5. If the RADIUS server returns authentication acceptance information in Step (3), the RADIUS client sends an accounting start request packet to the RADIUS server immediately.
6. The RADIUS server returns the accounting start response packet, indicating accounting start.
7. The user stops accessing network resources and requests the RADIUS client to disconnect the network connection.
8. The RADIUS client transmits the accounting end request packet to the RADIUS server.
9. The RADIUS server returns the accounting end response packet, indicating accounting end.
10. The user is disconnected and cannot access network resources.

Related Configuration

Configuring RADIUS Server Parameters

No RADIUS server is configured by default.

You can run the **radius-server host** command to configure a RADIUS server.

At least one RADIUS server must be configured so that RADIUS services run normally.

Configuring the AAA Authentication Method List

No AAA authentication method list is configured by default.

You can run the **aaa authentication** command to configure a method list for different user types and select **group radius** when setting the authentication method.

The RADIUS authentication can be conducted only after the AAA authentication method list of relevant user types is configured.

Configuring the AAA Authorization Method List

No AAA authorization method list is configured by default.

You can run the **aaa authorization** command to configure an authorization method list for different user types and select **group radius** when setting the authorization method.

The RADIUS authorization can be conducted only after the AAA authorization method list of relevant user types is configured.

Configuring the AAA Accounting Method List

No AAA accounting method list is configured by default.

You can run the **aaa accounting** command to configure an accounting method list for different user types and select **group radius** when setting the accounting method.

The RADIUS accounting can be conducted only after the AAA accounting method list of relevant user types is configured.

2.3.2 Source Address of RADIUS Packets

Specify the source IP address used by a RADIUS client to transmit packets to a RADIUS server.

Working Principle

When configuring RADIUS, specify the source IP address to be used by a RADIUS client to transmit RADIUS packets to a RADIUS server, in an effort to reduce the workload of maintaining a large amount of NAS information on the RADIUS server.

Related Configuration

The global routing is used to determine the source address for transmitting RADIUS packets by default.

Run the **ip radius source-interface** command to specify the source interface for transmitting RADIUS packets. The device uses the first IP address of the specified interface as the source address of RADIUS packets.

2.3.3 RADIUS Timeout Retransmission

Working Principle

After a RADIUS client transmits a packet to a RADIUS server, a timer is started to detect the response of the RADIUS server. If the RADIUS server does not respond within a certain period of time, the RADIUS client retransmits the packet.

Related Configuration

↘ Configuring the RADIUS Server Timeout Time

The default timeout time is 5 seconds.

You can run the **radius-server timeout** command to configure the timeout time. The value ranges from 1 second to 1,000 seconds.

The response time of a RADIUS server is relevant to its performance and the network environment. Set an appropriate timeout time according to actual conditions.

↘ Configuring the Retransmission Count

The default retransmission count is 3.

You can run the **radius-server retransmit** command to configure the retransmission count. The value ranges from 1 to 100.

↘ Configuring Whether to Retransmit Accounting Update Packets

Accounting update packets are not retransmitted by default.

You can run the **radius-server account update retransmit** command to configure retransmission of accounting update packets for authenticated users.

2.3.4 RADIUS Server Accessibility Detection

Working Principle

A RADIUS client actively detects whether a RADIUS server is reachable and maintains the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.

Related Configuration

↘ Configuring the Criteria for the Device to Judge That a RADIUS Server Is Unreachable

The default criteria configured for judging that a RADIUS server is unreachable meet the two conditions simultaneously: 1. The device does not receive a correct response packet from the RADIUS security server within 60 seconds. 2. The device transmits the request packet to the same RADIUS security server for consecutive 10 times.

You can run the **radius-server dead-criteria** command to configure the criteria for the device to judge that the RADIUS security server is unreachable.

↘ Configuring the Test User Name for Actively Detecting the RADIUS Security Server

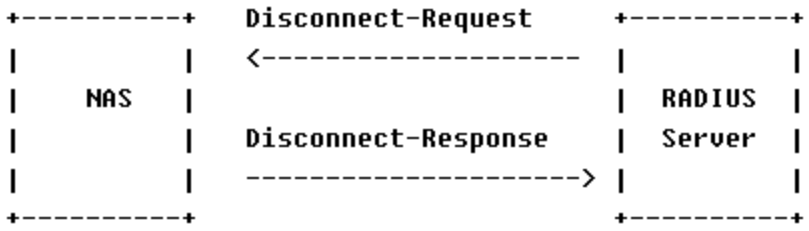
No test user name is specified for actively detecting the RADIUS security server by default.

You can run the **radius-server host x.x.x.x test username xxx** command to configure the test user name.

2.3.5 RADIUS Forced Offline

Working Principle

Figure 2-3 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol



The preceding figure shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request message to UDP Port 3799 of the device. After processing, the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

Related Configuration

N/A

2.4 Configuration

Configuration	Description and Command	
RADIUS Basic Configuration	(Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.	
	radius-server host	Configures the IP address of the remote RADIUS security server.
	radius-server key	Configures the shared key for communication between the device and the RADIUS server.
	radius-server retransmit	Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-server timeout	Configures the waiting time, after which the device retransmits a request.
	radius-server account update retransmit	Configures retransmission of accounting update packets for authenticated users.
	ip radius source-interface	Configures the source address of RADIUS packets.
Configuring the RADIUS Attribute Type	(Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.	

Configuration	Description and Command	
	radius-serverattribute31	Configures the MAC address format of RADIUS attribute No. 31 (Calling-Station-ID).
	radius-server attribute class	Configures the parsing mode of the RADIUS Class attribute.
	radius attribute	Configures the RADIUS private attribute type.
	radius set qoscos	Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the *Configuring QoS*.
	radius support cui	Configures the device to support the CUI attribute.
	radius-server authentication attribute	Configures whether RADIUS authentication request packets carry a specified attribute.
	radius-server account attribute	Configures whether RADIUS accounting request packets carry a specified attribute.
	radius-server authentication vendor	Configures whether RADIUS authentication request packets carry the private attributes of other vendors.
	radius-server account vendor	Configures whether RADIUS accounting request packets carry the private attributes of other vendors.
Configuring RADIUS Accessibility Detection	(Optional) It is used to detect whether a RADIUS server is reachable and maintain the accessibility of the RADIUS server.	
	radius-server dead-criteria	Configures the global criteria for judging that a RADIUS security server is unreachable.
	radius-server deadtime	Configures the duration for the device to stop transmitting request packets to an unreachable RADIUS server.
	radius-server host	Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.

2.4.1 RADIUS Basic Configuration

Configuration Effect

- RADIUS authentication, authorization, and accounting can be conducted after RADIUS basic configuration is complete.

Notes

- Before configuring RADIUS on the device, ensure that the network communication of the RADIUS server is in good condition.
- When running the **ip radius source-interface** command to configure the source address of RADIUS packets, ensure that the device of the source IP address communicates with the RADIUS server successfully.
- When conducting RADIUS IPv6 authentication, ensure that the RADIUS server supports RADIUS IPv6 authentication.

Configuration Steps

Configuring the Remote RADIUS Security Server

- Mandatory.
- Configure the IP address, authentication port, accounting port, and shard key of the RADIUS security server.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

- Optional.
- Configure a shared key in global configuration mode for servers without a shared key.

The shared key on the device must be consistent with that on the RADIUS server.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

- Optional.
- Configure the request transmission count, after which the device confirms that a RADIUS server is unreachable, according to the actual network environment.

Configuring the Waiting Time, After which the Device Retransmits a Request

- Optional.
- Configure the waiting time, after which the device retransmits a request, according to the actual network environment.

In an 802.1X authentication environment that uses the RADIUS security protocol, if a network device serves as the 802.1X authenticator and Hostname SU is used as the 802.1X client software, it is recommended that **radius-server timeout** be set to 3 seconds (the default value is 5 seconds) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

- Optional.
- Determine whether to enable the function of retransmitting accounting update packets of authenticated users according to actual requirements.

Configuring the Source Address of RADIUS Packets

- Optional.
- Configure the source address of RADIUS packets according to the actual network environment.

Configuring the Encapsulation Format of a Compatible User Name

- Optional.
- Configure the encapsulation format of a compatible user name as needed.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to confirm that the device communicates with the RADIUS server over the RADIUS protocol.

Related Commands

Configuring the Remote RADIUS Security Server

Command	**radius-server host** { *ipv4-address* | *ipv6-address*} [**auth-port***port-number*] [**acct-port***port-number*][**test username***name* [**idle-time***time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the RADIUS security server. *Ipv6-address*: Indicates the IPv6 address of the RADIUS security server. **auth-port***port-number*: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct identity authentication. **acct-port** *port-number*: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct accounting. **test username** *name*: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection. **idle-time***time*: Indicates the interval for the device to transmit test packets to a reachable RADIUS security server. The default value is 60 minutes. The value ranges from 1 minute to 1,440 minutes (24 hours). **ignore-auth-port**: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default. **ignore-acct-port**: Disables the function of detecting the accounting port of the RADIUS security server. It is enabled by default. **key**[**0** | **7**] *text-string* : Configures the shared key of the server. The global shared key is used if it is not configured. The configured key is displayed as "*" and you are required to enter the same key twice. If the entered keys are inconsistent, you need to re-enter the key. If inconsistency occurs for five consecutive times, the configuration will fail.
Command Mode	Global configuration mode
Usage Guide	A RADIUS security server must be defined to implement the AAA security service by using RADIUS. You can run the **radius-server host** command to define one or more RADIUS security servers.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

Command	**radius-server key** [**0** | **7**]*text-string*
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7**indicates simple encryption. The default value is **0**.
Command Mode	Global configuration mode
Usage Guide	A shared key is the basis for correct communication between the device and the RADIUS security server.

	The same shared key must be configured on the device and RADIUS security server so that they can communicate with each other successfully.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

Command	**radius-server retransmit***retries*
Parameter Description	*retries*: Indicates the RADIUS retransmission count. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count. There is an interval between consecutive two retransmissions.

Configuring the Waiting Time, After which the Device Retransmits a Request

Command	**radius-server timeout***seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the packet retransmission timeout time.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

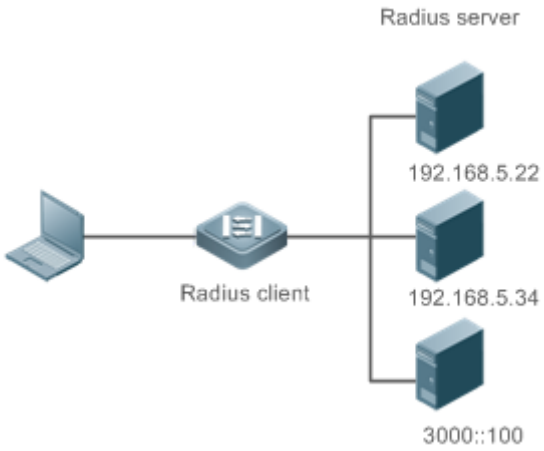
Command	**radius-server account update retransmit**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure retransmission of accounting update packets for authenticated users. Accounting update packets are not retransmitted by default. The configuration does not affect users of other types.

Configuring the Encapsulation Format of a Compatible User Name

Command	**radius user-name compatible**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the function is enabled, the user name in a RADIUS packet is encapsulated using the format sent by the client, instead of UTF-8.

Configuration Example

↘ Using RADIUS Authentication, Authorization, and Accounting for Login Users

Scenario **Figure 2-4**	
Configuration Steps	● Enable AAA. ● Configure the RADIUS server information. ● Configure to use the RADIUS authentication, authorization, and accounting methods. ● Apply the configured authentication method on the interface.
RADIUS Client	Hostname#configure terminal Hostname (config)#aaa new-model Hostname (config)# radius-server host 192.168.5.22 Hostname (config)#radius-server host 3000::100 Hostname (config)# radius-server key aaa Hostname (config)#aaa authentication login test group radius Hostname (config)#aaa authorizationexectest group radius Hostname (config)#aaa accountingexectest start-stop group radius Hostname (config)# line vty 0 4 Hostname (config-line)#login authentication test Hostname (config-line)# authorization exec test Hostname (config-line)# accounting exec test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. After obtaining a certain access level granted by the server, only run commands under this access level. Display the authentication log of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the

	accounting information on the user on the RADIUS server.
	Hostname#show running-config ! radius-server host 192.168.5.22 radius-server host 3000::100 radius-server key aaa aaa new-model aaa accounting exec test start-stop group radius aaa authorization exec test group radius aaa authentication login test group radius no service password-encryption iptcp not-send-rst ! vlan 1 ! line con 0 line vty 0 4 accounting exec test authorization exec test login authentication test !

Common Errors

- The key configured on the device is inconsistent with that configured on the server.
- No method list is configured.

2.4.2 Configuring the RADIUS Attribute Type

Configuration Effect

- Define the attribute processing adopted when the device encapsulates and parses RADIUS packets.

Notes

- Private attributes involved in "Configuring the RADIUS Attribute Type" refer to private attributes.

Configuration Steps

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

- Optional.
- Set the MAC address format of **Calling-Station-Id** to a type supported by the server.

Configuring the Parsing Mode of the RADIUS Class Attribute

- Optional.
- Configure the parsing mode of the Class attribute according to the server type.

Configuring the RADIUS Private Attribute Type

- Optional.
- If the server is an application server, the RADIUS private attribute type needs to be configured.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

- Optional.
- Set the private attribute **port-priority** issued by the server to the COS value of an interface as required.

Configures the Device to Support the CUI Attribute

- Optional.
- Configure whether the device supports the RADIUS CUI attribute as required.

Configuring the Mode of Parsing Private Attributes by the Device

- Optional.
- Configure the index of a private attribute parsed by the device as required.

Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

- Optional.
- Configure whether to specify the attribute type for RADIUS authentication request packets as required.

Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute

- Optional.
- Configure whether to specify the attribute type for RADIUS accounting request packets as required.

Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor

- Optional.
- Configure whether RADIUS authentication request packets carry the private attribute of a specified vendor as required.

Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor

- Optional.
- Configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

- Optional.
- Configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Configuring the Nas-Port-Id Encapsulation Format for RADIUS Packets

- Optional.
- In either QINQ or non-QINQ scenarios, configure the nas-nort-id encapsulation format for RADIUS packets. By default, the packets are encapsulated in the normal format.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to display the MAC address format of Calling-Station-Id.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that the CUI attribute is correctly parsed by the device.

Related Commands

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

Command	**radius-server attribute 31 mac format** {**ietf	normal	unformatted** }
Parameter Description	**ietf**: Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC. normal: Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac. **unformatted**: Indicates the format without separators. This format is used by default. Example: 00d0f83322ac.
Command Mode	Global configuration mode
Usage Guide	Some RADIUS security servers (mainly used for 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the MAC address format of Calling-Station-ID to IETF.

Configuring the Parsing Mode of the RADIUS Class Attribute

Command	**radius-server attribute class user-flow-control**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command if the server needs to issue the rate limit value by using the Class attribute.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

Command	**radius set qos cos**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to use the issued QoS value as the CoS value. The QoS value is used as the DSCP value by default.

Configures the Device to Support the CUI Attribute

Command	**radius support cui**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to enable the RADIUS-compliant device to support the CUI attribute.

Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

Command	**radius-server authentication attribute** *type* **package** **radius-server authentication attribute** *type* **unpackage**
Parameter Description	***type***: Indicates the RADIUS attribute type. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	Use this command to specify the attribute to be carried in authentication request packets.

Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute

Command	**radius-server account attribute** *type* **package** **radius-server account attribute** *type* **unpackage**
Parameter Description	***type***: Indicates the RADIUS attribute type. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	Use this command to specify the attribute to be carried in accounting request packets.

Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor

Command	**radius-server authentication vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to **cmcc**, **Microsoft**, or **cisco**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether authentication request packets carry the private attribute of a specified vendor.

Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor

Command	**radius-server account vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to **cmcc**, **Microsoft**, or **cisco**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether accounting request packets carry the private attribute of a specified vendor.

Configuration Example

Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	● Configure the MAC address format of RADIUS Calling-Station-Id. ● Configure the RADIUS private attribute type. ● Set the QoS value issued by the RADIUS server as the COS value of the interface. ● Configure the RADIUS function to support the CUI attribute. ● Configure the device to support private attributes of other vendors. ● Configure authentication requests not to carry the NAS-PORT-ID attribute. ● Configure accounting requests to carry the CMCC private attribute. ● Configure the RAIUDS server not to parse Cisoc's private attributes contained in packets. ● Configure application of the nas-port-id encapsulation format in a QINQ scenario.
	Hostname(config)#radius-server attribute 31 mac format ietf Hostname(config)#radius attribute 16 vendor-type 211 Hostname(config)#radiussetqoscos Hostname(config)#radiussupport cui Hostname(config)#radius-server authentication attribute 87 unpackage

	Hostname(config)#radius-server account vendor cmcc package
Verification	Conduct packet capture or display debug information of the device to check whether the RADIUS standard attributes and private attributes are encapsulated/parsed correctly.

2.4.3 Configuring RADIUS Accessibility Detection

Configuration Effect

The device maintains the accessibility status of each configured RADIUS server: reachable or unreachable. The device will not transmit authentication, authorization, and accounting requests of access users to an unreachable RADIUS server unless all the other servers in the same RADIUS server group as the unreachable server are all unreachable.

The device actively detects a specified RADIUS server. The active detection function is disabled by default. If the active detection function is enabled for a specified RADIUS server, the device will, according to the configuration, periodically transmits detection requests (authentication requests or accounting requests) to the RADIUS server. The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the active detection interval of the reachable RADIUS server (the default value is 60 minutes).
- For an unreachable RADIUS server, the interval is always 1 minute.

Notes

All the following conditions need to be met before the active detection function is enabled for a specified RADIUS server:

- The test user name of the RADIUS server is configured on the device.
- At least one tested port (authentication port or accounting port) of the RADIUS server is configured on the device.

If the following two conditions are all met, it is deemed that a reachable RADIUS server becomes unreachable:

- After the previous correct response is received from the RADIUS server, the time set in **radius-server dead-criteria time** *seconds* has elapsed.
- After the previous correct response is received from the RADIUS server, the count that the device transmits requests to the RADIUS server but fails to receive correct responses (including retransmission) reaches the value set in **radius-server dead-criteria tries** *number*.

If any of the following conditions is met, it is deemed that an unreachable RADIUS server becomes reachable:

- The device receives correct responses from the RADIUS server.
- The duration that the RADIUS server is in the unreachable state exceeds the time set in **radius-server deadtime** and the active detection function is disabled for the RADIUS server.
- The authentication port or accounting port of the RADIUS server is updated on the device.

Configuration Steps

↘ **Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable**

- Mandatory.
- Configuring the global criteria for judging that a RADIUS security server is unreachable is a prerequisite for enabling the active detection function.

Configuring the IP Address of the Remote RADIUS Security Server, Authentication Port, Accounting Port, and Active Detection Parameters

- Mandatory.
- Configuring active detection parameters of the RADIUS server is a prerequisite for enabling the active detection function.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

- Optional.
- The configured duration for the device to stop transmitting request packets to an unreachable RADIUS server takes effect only when the active detection function is disabled for the RADIUS server.

Verification

- Run the **show radius server** command to display the accessibility information of each RADIUS server.

Related Commands

Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

Command	**radius-server dead-criteria** { **time***seconds* [**tries***number*] | **tries***number* }
Parameter Description	**time***seconds*: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds. **tries***number*: Indicates the consecutive request timeout count. If the timeout count of request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	If a RADIUS security server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS security server is unreachable. Users can use this command to adjust parameter values in the duration condition and consecutive request timeout count condition.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

Command	**Radius-server deadtime** *minutes*
Parameter	*minutes*: Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS

Description	security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).
Command Mode	Global configuration mode
Usage Guide	If the active detection function is enabled for a RADIUS security server on the device, the time parameter in **radius-server deadtime** does not take effect on the RADIUS server. If the active detection function is disabled for a RADIUS security server, the device automatically restores the RADIUS security server to the reachable state when the duration that the RADIUS security server is in the unreachable state exceeds the time specified in **radius-server deadtime**.

Configuration Example

↘ Configuring Accessibility Detection on the RADIUS Server

Scenario **Figure 2-5**	
Configuration Steps	● Configure the global criteria for judging that a RADIUS security server is unreachable. ● Configure the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.
RADIUS Client	`Hostname(config)#radius-server dead-criteria time120 tries 5` `Hostname(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90`
Verification	Disconnect the network communication between the device and the server with the IP address of 192.168.5.22.Conduct RADIUS authentication through the device. After 120 seconds, run the **show radius server** command to check that the server state is **dead**.

	`Hostname#show running-config`
	`...`
	`radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90`
	`radius-server dead-criteria time 120 tries 5`
	`...`

2.5 Monitoring

Displaying

Description	Command

Description	Command
Displays global parameters of the RADIUS server.	**show radius parameter**
Displays the configuration of the RADIUS server.	**show radius server**
Displays statistics relevant to the RADIUS dynamic authorization extension function.	**show radius dynamic-authorization-extension statistics**
Displays statistics relevant to RADIUS authentication.	**show radius auth statistics**
Displays statistics relevant to RADIUS accounting.	**show radius acct statistics**
Displays configuration of RADIUS server groups.	**show radius group**
Displays RADIUS standard attributes.	**Show radius attribute**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the RADIUS event.	**debugradiusevent**
Debugs RADIUS packet printing.	**debugradiusdetail**
Debugs the RADIUS dynamic authorization extension function.	**debug radiusextension event**
Debugs the RADIUS dynamic authorization extension packet printing.	**debug radius extension detail**

3 Configuring TACACS+

3.1 Overview

TACACS+ is a security protocol enhanced in functions based on the Terminal Access Controller Access Control System (TACACS) protocol. It is used to implement the authentication, authorization, and accounting (AAA) of multiple users.

Protocols and Standards

- RFC 1492 Terminal Access Controller Access Control System

3.2 Applications

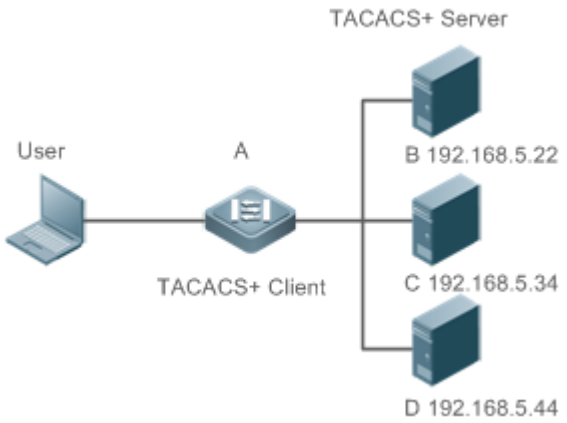
Application	Description
Managing and Controlling Login of End Users	Password verification and authorization need to be conducted on end users.

3.2.1 Managing and Controlling Login of End Users

Scenario

TACACS+ is typically applied in the login management and control of end users. A network device serves as the TACACS+ client and sends a user name and password to the TACACS+ server for verification. The user is allowed to log in to the network device and perform operations after passing the verification and obtaining authorization. See the following figure.

Figure 3-1



Remarks	• A is a client that initiates TACACS+ requests. • B, C, and D are servers that process TACACS+ requests.

Deployment

- Start the TACACS+ server on Server B, Server C, and Server D, and configure information on the access device (Device A) so that the servers provide TACACS+-based AAA function for the access device. Enable the AAA function on Device A to start authentication for the user login.
- Enable the TACACS+ client function on Device A, add the IP addresses of the TACACS+ servers (Server B, Server C, and Server D) and the shared key so that Device A communicates with the TACACS+ servers over TACACS+ to implement the AAA function.

3.3 Features

Basic Concepts

Format of TACACS+ Packets

Figure 3-2

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

- Major Version: Indicates the major TACACS+ version number.
- Minor Version: Indicates the minor TACACS+ version number.
- Packet Type: Indicates the type of packets, with the options including:
  TAC_PLUS_AUTHEN: = 0x01 (authentication);
  TAC_PLUS_AUTHOR: = 0x02 (authorization);
  TAC_PLUS_ACCT: = 0x03 (accounting)
- Sequence Number: Indicates the 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 subsequent each data packet increases by one. Therefore, the client sends data packets only with an odd sequence number and TACACS+ Daemon sends packets only with an even sequence number.
- Flags: Contains various bitmap format flags. One of the bits in the value specifies whether data packets need to be encrypted.
- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets are encrypted for transmission on a network.

Overview

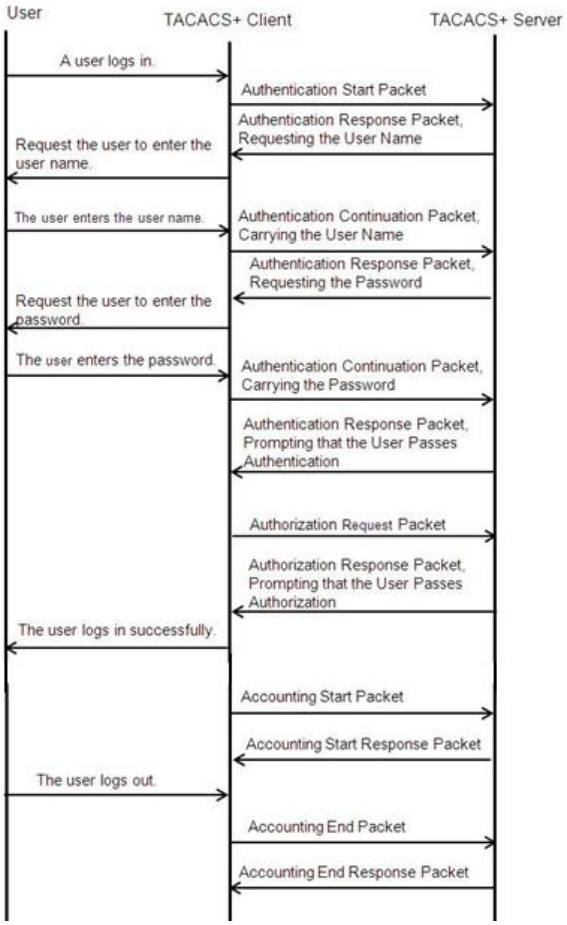
Feature	Description
TACACS+ Authentication, Authorization, and Accounting	Conducts authentication, authorization, and accounting on end users.

3.3.1 TACACS+ Authentication, Authorization, and Accounting

Working Principle

The following figure uses basic authentication, authorization, and accounting of user login to describe interaction of TACACS+ data packets.

Figure 3-3



The entire basic message interaction process includes three sections:

1. The authentication process is described as follows:
   1) A user requests to log in to a network device.
   2) After receiving the request, the TACACS+ client sends an authentication start packet to the TACACS+ server.
   3) The TACACS+ server returns an authentication response packet, requesting the user name.

4) The TACACS+ client requests the user to enter the user name.

5) The user enters the login user name.

6) After receiving the user name, the TACACS+ client sends an authentication continuation packet that carries the user name to the TACACS+ server.

7) The TACACS+ server returns an authentication response packet, requesting the login password.

8) The TACACS+ client requests the user to enter the login password.

9) The user enters the login password.

10) After receiving the login password, the TACACS+ client sends an authentication continuation packet that carries the login password to the TACACS+ server.

11) The TACACS+ server returns an authentication response packet, prompting that the user passes authentication.

Configuration	Description and Command	
Configuring TACACS+ Basic Functions	(Mandatory) It is used to enable the TACACS+ security service.	
	tacacs-server host	Configures the TACACS+ server.
	tacacs-server key	Specifies the key shared by the server and network device.
	tacacs-server timeout	Configures the global waiting timeout time of the TACACS+ server for communication between a network device and the TACACS+ server.
Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+	(Optional) It is used to separately process authentication, authorization, and accounting requests.	
	aaa group server tacacs+	Configures TACACS+ server groups and divides TACACS+ servers into different groups.
	server	Adds servers to TACACS+ server groups.

2. The user authorization starts after successful authentication:

   1) The TACACS+ client sends an authorization request packet to the TACACS+ server.

   2) The TACACS+ server returns an authorization response packet, prompting that the user passes authorization.

   3) After receiving the authorization success packet, the TACACS+ client outputs the network device configuration screen for the user.

3. Accounting and audit need to be conducted on the login user after successful authorization:

   1) The TACACS+ client sends an accounting start packet to the TACACS+ server.

   2) The TACACS+ server returns an accounting response packet, prompting that the accounting start packet has been received.

3) The user logs out.

4) The TACACS+ client sends an accounting end packet to the TACACS+ server.

5) The TACACS+ server returns an accounting response packet, prompting that the accounting end packet has been received.

3.4 Configuration

3.4.1 Configuring TACACS+ Basic Functions

Configuration Effect

- The TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the method of using TACACS+ to implement TACACS+ authentication, authorization, and accounting.
- When authentication, authorization, and accounting operations are performed, TACACS+ initiates the authentication, authorization, and accounting requests to configured TACACS+ servers according to the configured sequence. If response timeout occurs on a TACACS+ server, TACACS+ traverses the TACACS+ server list in sequence.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

↘ Enabling AAA

- Mandatory. The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

Command	aaa new-model
Parameter Description	N/A
Defaults	The AAA function is disabled.
Command Mode	Global configuration mode
Usage Guide	The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

↘ Configuring the IP Address of the TACACS+ Server

- Mandatory. Otherwise, a device cannot communicate with the TACACS+ server to implement the AAA function.

Command	**tacacs-server host** {*ipv4-address* | *ipv6-address*} [**port***integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server. **port***integer*: Indicates the TCP port used for TACACS+ communication. The default TCP port is 49. **timeout** *integer*: Indicates the timeout time of the communication with the TACACS+ server. The global timeout time is used by default. **key** [**0** | **7**] *text-string*: Indicates the shared key of the server. The global key is used if it is not configured. An encryption type can be specified for the configured key. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.
Defaults	No TACACS+ server is configured.
Command Mode	Global configuration mode
Usage Guide	1. You can specify the shared key of the server when configuring the IP address of the server. If no shared key is specified, the global key configured using the **tacacs-server key** command is used as the shared key of the server. The shared key must be completely the same as that configured on the server. 2. You can specify the communication port of the server when configuring the IP address. 3. You can specify the communication timeout time of the server when configuring the IP address.

Configuring the Shared Key of the TACACS+ Server

- Optional.
- If no global communication protocol is configured using this command, set **key** to specify the shared key of the server when running the **tacacs-server host** command to add server information. Otherwise, a device cannot communicate with the TACACS+ server.
- If no shared key is specified by using **key** when you run the **tacacs-server host** command to add server information, the global key is used.

Command	**tacacs-server** [**key** [**0** | **7**] *text-string*]
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7** indicates simple encryption.
Defaults	No shared key is configured for any TACACS+ server.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure a global shared key for servers. To specify a different key for each server, set **key** when running the **tacacs-server host** command.

Configuring the Timeout Time of the TACACS+ Server

- Optional.
- You can set the timeout time to a large value when the link between the device and the server is unstable.

Command	**tacacs-server timeout***seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the global server response timeout time. To set different timeout time for each server, set **timeout** when running the **tacacs-server host** command.

Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable the device to interact with the TACACS+ server and conduct packet capture to check the TACACS+ interaction process between the device and the TACACS+ server.
- View server logs to check whether the authentication, authorization, and accounting are normal.

Configuration Example

Using TACACS+ for Login Authentication

Scenario Figure 3-4	
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure the method of using TACACS+ for authentication. ● Apply the configured authentication method on an interface.
A	Hostname# configure terminal Hostname(config)# aaa new-model Hostname(config)# tacacs-server host 192.168.5.22 Hostname(config)# tacacs-server key aaa Hostname(config)# aaa authentication login test group tacacs+

	Hostname(config)# line vty 0 4 Hostname(config-line)# login authentication test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. View the authentication log of the user on the TACACS+ server.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- No method list is configured.

3.4.2 Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+

Configuration Effect

- The authentication, authorization, and accounting in the security service are processed by different TACACS+ servers, which improves security and achieves load balancing to a certain extent.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

↘ Configuring TACACS+ Server Groups

- Mandatory. There is only one TACACS+ server group by default, which cannot implement separate processing of authentication, authorization, and accounting.
- Three TACACS+ server groups need to be configured for separately processing authentication, authorization, and accounting.

Command	**aaa group server tacacs+***group-name*
Parameter Description	*group-name*: Indicates the name of a group. A group name cannot be radius or tacacs+, which are the names of embedded groups.
Defaults	No TACACS+ server group is configured.
Command Mode	Global configuration mode
Usage Guide	Group TACACS+ servers so that authentication, authorization, and accounting are completed by different

	server groups.

Adding Servers to TACACS+ Server Groups

- Mandatory. If no server is added to a server group, a device cannot communicate with TACACS+ servers.
- In server group configuration mode, add the servers that are configured using the **tacacs-server host** command.

Command	**server {***ipv4-address* | *ipv6-address*}
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server.
Defaults	No server is configured.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. For the address of a server configured in a TACACS+ server group, the server must be configured using the **tacacs-server host** command in global configuration mode. If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to another server in the server group.

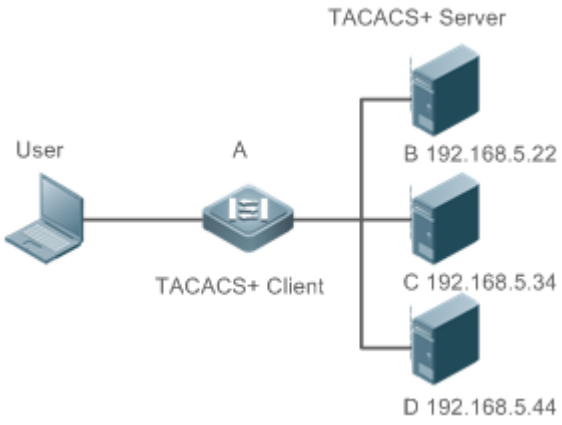
Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable a device to interact with TACACS+ servers. Conduct packet capture, check that the authentication, authorization, and accounting packets are interacted with different servers, and check the source addresses in packets.

Configuration Example

Configuring Different TACACS+ Server Groups for Separately Processing Authentication, Authorization, and Accounting

Scenario **Figure 3-5**	

Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ authentication requests. ● C is a server that processes TACACS+ authorization requests. ● D is a server that processes TACACS+ accounting requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure TACACS+ server groups. ● Add servers to TACACS+ server groups. ● Configure the method of using TACACS+ for authentication. ● Configure the method of using TACACS+ for authorization. ● Configure the method of using TACACS+ for accounting. ● Apply the configured authentication method on an interface. ● Apply the configured authorization method on an interface. ● Apply the configured accounting method on an interface.
	Hostname# configure terminal Hostname(Hostname(config)# aaa new-model Hostname(config)# tacacs-server host 192.168.5.22 Hostname(config)# tacacs-server host 192.168.5.34 Hostname(config)# tacacs-server host 192.168.5.44 Hostname(config)# tacacs-server key aaa Hostname(config)# aaa group server tacacs+ tacgrp1 Hostname(config-gs-tacacs)# server 192.168.5.22 Hostname(config-gs-tacacs)# exit Hostname(config)# aaa group server tacacs+ tacgrp2 Hostname(config-gs-tacacs)# server 192.168.5.34 Hostname(config-gs-tacacs)# exit Hostname(config)# aaa group server tacacs+ tacgrp3 Hostname(config-gs-tacacs)# server 192.168.5.44 Hostname(config-gs-tacacs)# exit Hostname(config)# aaa authentication login test1 group tacacs+ Hostname(config)# aaa authentication enable default group tacgrp1 Hostname(config)# aaa authorization exec test2 group tacgrp2 Hostname(config)# aaa accounting commands 15 test3 start-stop group tacgrp3

	Hostname(config)# line vty 0 4 Hostname(config-line)# login authentication test1 Hostname(config-line)#authorization exec test2 Hostname(config-line)# accounting commands 15 test3
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. Enter the **enable** command and enter the correct **enable** password to initiate **enable** authentication. Enter the privilege EXEC mode after passing the authentication. Perform operations on the device and then exit the device. View the authentication log of the user on the server with the IP address of 192.168.5.22. View the **enable** authentication log of the user on the server with the IP address of 192.168.5.22. View the **exec** authorization log of the user on the server with the IP address of 192.168.5.34. View the command accounting log of the user on the server with the IP address of 192.168.5.44.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- Undefined servers are added to a server group.
- No method list is configured.

3.5 Monitoring

Displaying

Description	Command
Displays interaction with each TACACS+ server.	**show tacacs**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs TACACS+.	**debug tacacs+**

4 Configuring 802.1X

4.1 Overview

IEEE 802.1X is a standard for port-based network access control that provides secure access service for local area networks (LANs).

In IEEE 802-compliant LANs, users connecting to the network access devices (NASs) can access network resources without authentication and authorization, bringing security risks to the network. IEEE 802.1X was proposed to resolve security problems of such LANs.

802.1X supports three security applications: authentication, authorization, and accounting, which are called AAA.

- Authentication: Checks whether to allow user access and restricts unauthorized users.
- Authorization: Grants specified services to users and controls permissions of authorized users.
- Accounting: Records network resource status of users to provide statistics for charges.

802.1X can be deployed in a network to realize user authentication, authorization and other functions.

Protocols and Standards

- IEEE 802.1X: Port-Based Network Access Control

4.2 Applications

Application	Description
Wired 802.1X Authentication	To ensure secure admission on the campus network, 802.1X authentication is deployed on access switches.

4.2.1 Wired 802.1X Authentication

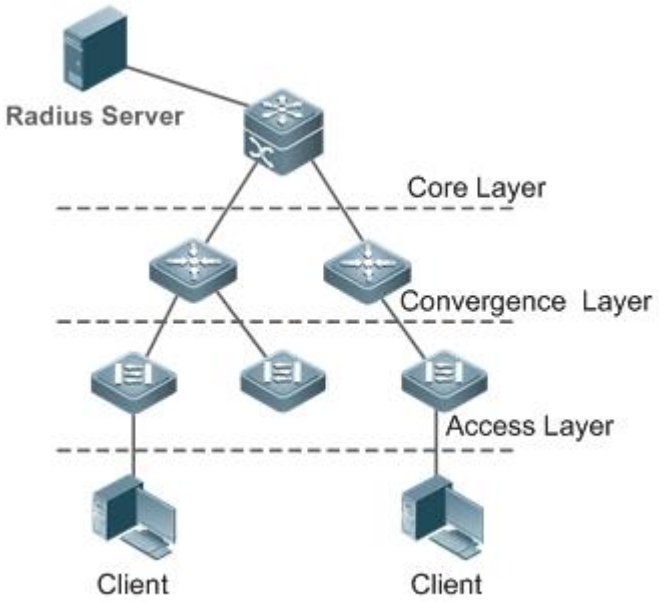
Scenario

The campus network is deployed at the access, convergence, and core layers. 802.1X is deployed on access switches connected to dormitories to perform secure admission. Dormitory users must pass 802.1X authentication before accessing the campus network.

As shown in Figure 4-1:

- User ends must be installed with 802.1X clients (which can come with the operating system, or other supplicants).
- Access switches support 802.1X.
- One or multiple Remote Authentication Dial-In User Service (RADIUS) servers perform authentication.

Figure 4-1



Remarks	The supplicant software installed on the user ends (or software coming with the operating system) performs 802.1X authentication. 802.1X authentication is deployed on access switches, convergence switches, or core switches. The RADIUS server runs the RADIUS server software to perform identity verification.

Deployment

- Enable 802.1X authentication on ports between access switches and users to make ports controllable. Only authenticated users on one port can access the network.
- Configure an AAA authentication method list so that 802.1X can adopt the appropriate method and authentication server.
- Configure RADIUS parameters to ensure proper communication between a switch and the RADIUS server. For details, see the *Configuring RDS*.
- If a RADIUS server is used, configure SNMP parameters to allow the RADIUS server to manage devices, such as querying and setting.
- Configure the port between the access switch and the RADIUS server as an uncontrolled port to ensure proper communication between them.
- Create an account on the RADIUS server, register the IP address of an access switch, and configure RADIUS-related parameters. Only in this case, can the RADIUS server respond to the requests of the switch.

4.2.2 MAB Auto Authentication

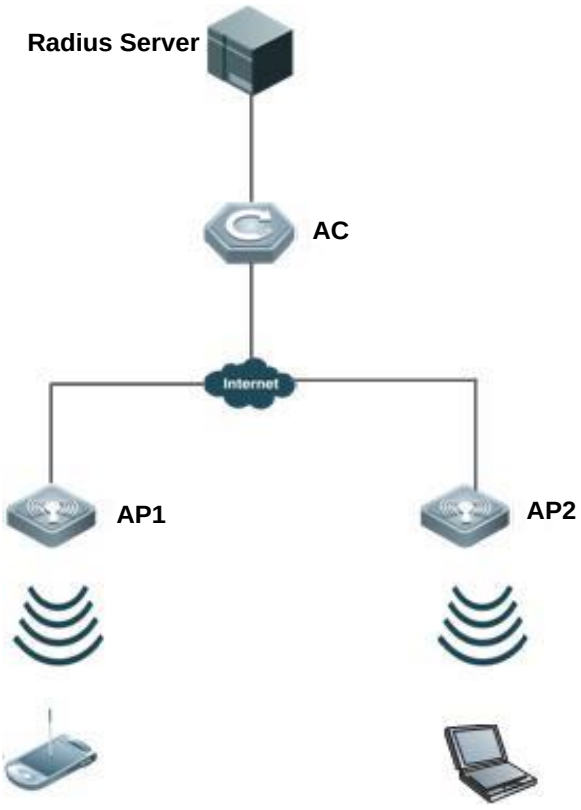
Scenario

MAC address bypass (MAB) auto authentication indicates that MAB authentication is performed together with Web authentication. In the original wireless Web authentication scenario, it is complained that the ease-to-use performance of Web authentication is poor. During each Web authentication, a user needs to associate the STA with an SSID, open the browser, and enter the user name and password. In addition, if the STA drops out of the network, the STA cannot automatically access the network again. To ensure that all Web authenticated STAs are always online and access the network imperceptibly, MAB auto authentication is proposed. After a STA passes Web authentication, the STA can access the network again imperceptibly without Web authentication.

As shown in Figure 4-2:

- Only the browser is mandatory on the client.
- The AC supports Web authentication and MAB authentication.
- One or multiple RADIUS servers provide authentication. In addition, the authentication server supports the authentication mode of using the MAC address as the user name and password.

Figure 4-2



Remarks	Wireless MAB authentication is triggered by a STA advertisement. When a STA is already online, MAB authentication will not be triggered again. If MAB authentication fails, it can be triggered again only after the STA

	goes offline and reconnects to the network.

Deployment

- Enable Web authentication, DOT1X authentication, and MAB authentication on the interface of the AC. MAB authentication can be performed only after DOT1X authentication is enabled. (For details about MAB authentication, see section 4.4.5 "Configuring MAB Auto Authentication". For details about Web authentication, see the WEB-AUTH-SCG document.)
- Configure an AAA authentication method list, so that a correct method and authentication server can be used for MAB/Web authentication. (For details about the AAA authentication method list configuration, see the AAA-SCG document.)
- Configure RADIUS parameters to ensure proper communication between the AC and the RADIUS server. In addition, configure the RADIUS server to support the authentication mode of using the MAC address as the user name and password. For details about the RADIUS configuration, see the corresponding configuration guide.
- If a RADIUS server is used, configure SNMP parameters to allow the RADIUS server to perform operations such as querying and setting on the AP.
- Create an account on the RADIUS server, register the IP address of the AC, and configure RADIUS-related parameters. The RADIUS server can respond to the requests of the AP and AC only after the foregoing settings are completed.

4.3 Features

Basic Concepts

User

In wired environment, 802.1X is a LAN-based protocol. It identifies users based on physical information but not accounts. In a LAN, a user is identified by the MAC address and VLAN ID (VID). Except them, all other information such as the account ID and IP address can be changed.

RADIUS

RADIUS is a remote authentication protocol defined in RFC2865, which get wide practice. Using this protocol, the authentication server can remotely deploy and perform authentication. During 802.1X deployment, the authentication server is remotely deployed, and 802.1X authentication information between the NAS and the authentication server is transmitted through RADIUS.

Timeout

During authentication, an NAS needs to communicate with the authentication client and server. If the authentication client or server times out, not responding within the time specified by 802.1X, authentication will fail. During deployment, ensure that the timeout specified by 802.1X is longer than that specified by RADIUS.

MAB

MAC address bypass (MAB) authentication means that the MAC address is used as the user name and password for authentication. Since the supplicant cannot be installed on some dumb ends such as network printers, use MAB to perform security control.

EAP

802.1X uses Extensible Authentication Protocol (EAP) to carry authentication information. Defined in RFC3748, EAP provides a universal authentication framework, in which multiple authentication modes are embedded, including Message Digest Algorithm 5 (MD5), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Transport Layer Security (TLS). 802.1X authentication supports various modes including MD5, CHAP, PAP, PEAP-MSCHAP, and TLS.

Authorization

Authorization means to bind specified services to authenticated users, such as IP address, VLAN, Access Control List (ACL), and Quality of Service (QoS).

Accounting

Accounting performs network audit on network usage duration and traffic for users, which facilitates network operation, maintenance, and management.

Some RADIUS servers such as SAM\SMP servers need to check the online/offline status based on accounting packets. Therefore, accounting must be enabled on these RADIUS servers.

Overview

Feature	Description
Authentication	Provides secure admission for users. Only authenticated users can access the network.
Authorization	Grants network access rights to authenticated users, such as IP address binding and ACL binding
Accounting	Provides online record audit, such as online duration and traffic.

4.3.1 Authentication

Authentication aims to check whether users are authorized and prevent unauthorized users from accessing the network. Users must pass authentication to obtain the network access permission. They can access the network only after the authentication server verifies the account. Before user authentication succeeds, only EAPOL packets (Extensible Authentication Protocol over LAN, 802.1X packets) can be transmitted over the network for authentication.

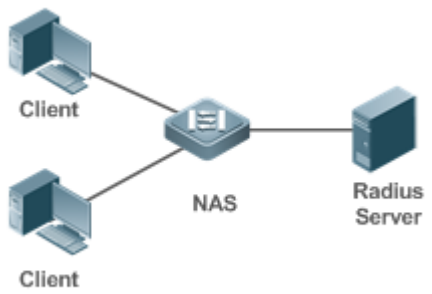
Working Principle

802.1X authentication is very simple. After a user submits its account information, the NAS sends the account information to the remote RADIUS server for identity authentication. If the authentication succeeds, the user can access the network.

Roles in Authentication

802.1X authentication involves three roles: supplicant, authenticator, and server. In real applications, their respective roles are client, network access server (NAS), and authentication server (mostly RADIUS server).

Figure 4-3



- Supplicant

The supplicant is the role of end users, usually a PC. It requests to access network services and replies to the request packets of the authenticator. The supplicant must run software compliant with the 802.1X standard. Except the typical 802.1X client support embedded in the operating system, the company has launched a supplicant compliant with the 802.1X.

- Authenticator

The authenticator is usually an NAS such as a switch access hotspot. It controls the network connection of a client based on the client's authentication status. As a proxy between the client and the authentication server, the authenticator requests the user name from the client, verifies the authentication information from the authentication server, and forwards it to the client. Except as the 802.1X authenticator, the so-called NAS also acts as a RADIUS Client. It encapsulates the replies of the client into the RADIUS-format packets and forwards the packets to the RADIUS server. After receiving the information from the RADIUS server, it interprets the information and forwards it to the client.

The authenticator has two types of ports: controlled port and uncontrolled port. Users connected to controlled ports can access network resources only when authenticated. Users connected to uncontrolled ports can directly access network resources without authentication. We can connect users to controlled ports to control users. Uncontrolled ports are mainly used to connect the authentication server to ensure proper communication between the authentication server and the NAS.

- Authentication server

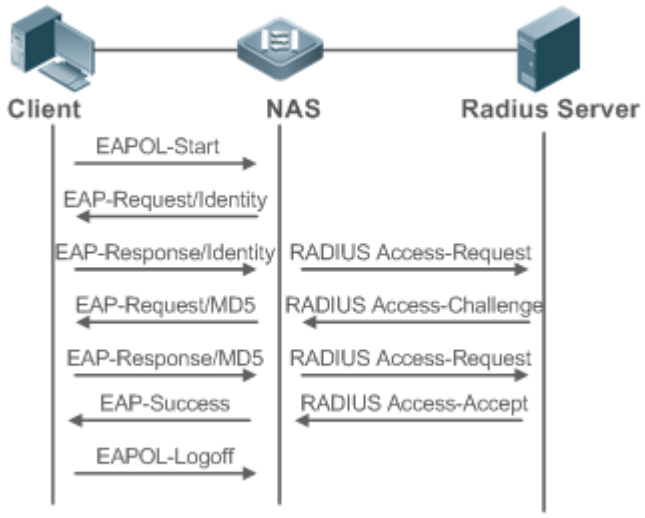
The authenticator server is usually an RADIUS server. It cooperates with the authenticator to provide authentication service for users. The authentication server saves the user names, passwords, and related authorization information. One server can provides authentication service for multiple authenticators to achieve centralized user management. The authentication server also manages accounting data received from authenticators. RADIUS servers compliant with 802.1X standard include Microsoft IAS/NPS, Free RADIUS Server, and Cisco ACS.

Authentication Process and Packet Exchange

The supplicant exchanges information with the authenticator through EAPOL while exchanges information with the authentication server through RADIUS. EAPOL is encapsulated on the MAC layer, with the type number of 0x888E. IEEE assigned a multicast MAC address 01-80-C2-00-00-03 for EAPOL to exchange packets during initial authentication. Supplicants may also use 01-D0-F8-00-00-03 to for initial authentication packets.

Figure 4-4 shows the typical authentication process of a wired user.

Figure 4-4



Authenticating User Status

802.1X determines whether a user on a port can access the network based on the authentication status of the port. The products extend the 802.1X and realizes access control based on users (identify a wired user by the MAC address and VLAN ID) by default. 802.1X can also be enabled in interface configuration mode. For details, see the chapter "Configuration."

All users on an uncontrolled port can access network resources, while users on a controlled port can access network resources only after authorized. When a user initiates authentication, its status remains Unauthorized and cannot access the network yet. After it passes authentication, its status changes to Authorized and can access network resources.

If the user connected to a controlled port does not support 802.1X, it will not respond to the NAS requesting the user name of the user. That means, the user remains Unauthorized and cannot access network resources.

In the case of 802.1X-enabled user and 802.1X-disabled NAS, if the user does not receive any responses after sending a specified number of EAPOL-Start packets, it regards the connected port uncontrolled and directly accesses network resources.

On 802.1X-enabled devices, all ports are uncontrolled by default. We can configure a port as controlled so that all users on this port have to be authorized.

If a user passes authentication (that is, the NAS receives a success packet from the RADIUS server), the user becomes Authorized and can freely access network resources. If the user fails in authentication, it remains Unauthorized and re-initiates authentication. If the communication between the NAS and the RADIUS server fails, the user remains Unauthorized and cannot access network resources.

When a user sends an EAPOL-LOGOFF packet, the user's status changes from Authorized to Unauthorized.

When a port of the NAS goes down, all users on this port will become Unauthorized.

When the NAS restarts, all users on it become Unauthorized.

Deploying the Authentication Server

802.1X authentication uses the RADIUS server as the authentication server. Therefore, when 802.1X secure admission is deployed, the RADIUS server also needs to be deployed. Common RADIUS servers include Microsoft IAS/NPS, Cisco ACS, and SAM/SMP. For details about the deployment procedure, see related software description.

Configuring Authentication Parameters

To use 802.1X authentication, enable 802.1X authentication on the access port and configure AAA authentication method list and RADIUS server parameters. To ensure the accessibility between the NAS and RADIUS server, the 802.1X server timeout should be longer than the RADIUS server timeout.

Supplicant

A user should start the supplicant to enter the user name and initiate authentication. If the operating system brings an own authentication client and the network is available, a dialog box will be displayed, asking the user to enter the user name. Different clients may have different implementation processes and Graphical User Interfaces (GUIs). It is recommended to use the supplicant as the authentication client. If other software is used, see related software description.

Offline

If a user does not want to access the network, it can choose to go offline by multiple approaches, such as powering off the device, connecting the port to the network, and offline function provided by some supplicants.

4.3.2 Authorization

After a user passes authentication, the NAS restricts the accessible network resources of the user in multiple approaches, such as binding the IP address and the MAC address, and specifying the maximum online time or period, accessible VLANs, and bandwidth limit.

Working Principle

Authorization means to bind the permissions with the users. A user is identified based on the MAC address and VLAN ID, as mentioned before. Besides MAC-VID binding, some other information such as the IP address and VLAN ID are bound with a user to implement authorization.

IP Authorization

802.1X does not support IP address identification. 802.1X authentication extends 802.1X to support IP-MAC binding, which is called IP authorization. IP authorization supports four modes:

Supplicant authorization: The IP address is provided by the supplicant.

RADIUS authorization: After successful authentication, the RADIUS server delivers the IP address to the NAS.

DHCP authorization: In such case, an authenticated user will initiate a DHCP request to obtain an IP address, and then bind the IP address with the MAC address of the client.

Mixed authorization: IP-MAC binding is configured for users in the following sequence: Supplicant authorization -> RADIUS authorization -> DHCP authorization. That is, the IP address provided by the supplicant preferred, then the IP address provided by the RADIUS server, and finally the IP address provided by DHCP.

ACL Authorization

After user authentication is complete, the authentication server delivers the ACL or ACE to users. The ACL must be configured on the authentication server before delivery while no extra configuration is required for ACE delivery. ACL authorization delivers the ACL based on RADIUS attributes such as standard attributes, our company's proprietary attributes, and Cisco-proprietary attributes. For details, see the software description related to the RADIUS server.

Kickoff

Used with SAM/SMP, 802.1X server can kick off online users who will be disconnected with the network. This function applies to the environment where the maximum online period and real-time accounting check function are configured.

4.3.3 Accounting

Accounting allows the network operators to audit the network access or fees of accessed users, including the online time and traffic.

Working Principle

Accounting is enabled on the NAS. The RADIUS server supports RFC2869-based accounting. When a user goes online, the NAS sends an accounting start packet to the RADIUS server which then starts accounting. When the user goes offline, the NAS sends an accounting end packet to the RADIUS server which then completes the accounting and generates a network fee accounting list. Different servers may perform accounting in different ways. Moreover, not all servers support accounting. Therefore, refer to the usage guide of the authentication server during actual deployment and accounting.

Accounting Start

After a user passes authentication, the accounting-enabled switch sends the RADIUS server an accounting start packet carrying user accounting attributes such as user name and accounting ID. After receiving the packet, the RADIUS server starts accounting.

Accounting Update

The NAS periodically sends Accounting Update packets to the RADIUS server, making the accounting more real-time. The accounting update interval can be provided by the RADIUS server or configured on the NAS.

Accounting End

After a user goes offline, the NAS sends the RADIUS server an accounting end packet carrying the online period and traffic of the user. The RADIUS server generates online records based on the information carried in this packet.

4.4 Configuration

Configuration	Description and Command	
Configuring 802.1X Basic Functions	(Mandatory) It is used to configure basic authentication and accounting.	
	aaa new-model	Enables AAA.
	aaa authentication dot1x	Configures an AAA authentication method list.
	aaa accounting network	Configures an AAA accounting method list.
	radius-server host	Configures the RADIUS server parameters.
	radius-server key	Configures the preshared key for communication between the NAS and the RADIUS server.
	dot1x port-control auto	Enables 802.1X authentication on a port.
Configuring 802.1X Parameters	(Optional) It is used to configure 802.1X parameters. Ensure that the 802.1X server timeout is longer than the RADIUS server timeout. Online client detection applies only to our company's supplicant.	
	dot1x re-authentication	Enables re-authentication.
	dot1x timeout re-authperiod	Configures the re-authentication interval.
	dot1x timeout tx-period	Configures the interval of EAP-Request/Identity packet retransmission.
	dot1x reauth-max	Configures the maximum times of EAP-Request/Identity packet retransmission.
	dot1x timeout supp-timeout	Configures the interval of EAP-Request/Challenge packet retransmission.
	dot1x max-req	Configures the maximum times of EAP-Request/Challenge packet retransmission.
	dot1x timeout server-timeout	Configures the authentication server timeout.
	dot1x timeout quiet-period	Configures the quiet period after authentication fails.
	dot1x auth-mode	Specifies the authentication mode (EAP/CHAP/PAP).
	dot1x client-probe enable	Enables online client detection.

	dot1x probe-timer interval	Configures the interval of online client detection.
	dot1x probe-timer alive	Configures the duration of online client detection.
Configuring Authorization	(Optional) It is used to configure authorization. Our company's supplicant should be used to perform supplicant authorization in IP authorization mode.	
	aaa authorization ip-auth-mode	Specifies the IP authorization mode.
	dot1x private-supplicant-only	Filters the clients except our company's clients.
	dot1x redirect	Enables Web Redirection for 2G Supplicant Deployment.
	snmp	Configures SNMP parameters. SAM/SMP can implement functions for 802.1X online users through SNMP. SNMP parameters should be configured to implement such functions.
Configuring MAB	(Optional) It is used to configure MAC Authentication Bypass (MAB). 802.1X authentication takes priority over MAB. MAB does not support IP authorization. Single-user MAB and multi-user MAB cannot be enabled at the same time. MAB adopts the PAP authentication mode. Ensure correct server configurations during deployment.	
	dot1x mac-auth-bypass	Enables single-user MAB.
	dot1x mac-auth-bypass multi-user	Enables multi-user MAB.
	dot1x multi-mab quiet-period	Configures the blocking period after multi-user MAB fails.
	dot1x mac-auth-bypass timeout-activity	Configures the timeout of MAB users.
	dot1x mac-auth-bypass violation	Enables MAB violation mode.
	dot1x mac-auth-bypass vlan	Configures VLAN-based MAB.
Configuring IAB	(Optional) It is used to configure Inaccessible Authentication Bypass (IAB).	
	dot1x critical	Enables IAB.
	dot1x critical recovery action reinitialize	Enables IAB recovery.
	dot1x critical vlan	Configures the IAB VLAN.
Configuring Port Control	**dot1x port-control-mode mac-based**	Enables the MAC-based control mode.
	dot1x port-control-mode port-based	Enables the port-based control mode.

	dot1x port-control-mode port-based single-host	Enables the single-user port-based control mode.
	dot1x stationarity enable	Disables migration of dynamic users.
Configuring Extended Functions	(Optional) It is used to configure active authentication requests on a port. (Optional) It is used to configure the authenticated client list. (Optional) It is used to enable 802.1X packet sending with the pseudo source MAC address. (Optional) It is used to configure multiple accounts for the same MAC address.	
	dot1x auto-req	Enables active authentication.
	dot1x auto-req packet-num	Configures the number of active authentication requests.
	dot1x auto-req user-detect	Enables user detection for active authentication.
	dot1x auto-req req-interval	Configures the interval of active authentication request.
	dot1x auth-address-table address	Configures the authenticatable client list.
	dot1x pseudo source-mac	Enables 802.1X packets sending with the pseudo source MAC address.
	dot1x multi-account enable	Enables multi-account authentication with one MAC address.
	dot1x valid-ip-acct enable	Enables IP-triggered accounting.
	dot1x valid-ip-acct timeout	Configures the timeout of obtaining IP addresses after users get authenticated. If timeout is reached, they will be kicked off.
	dot1x auth-with-order	Eanbles 802.1X precedence over MAB.
	dot1x user-name compatible	Configures compatibility for H3C 802.1X authentication clients and authentication servers.

4.4.1 Configuring 802.1X Basic Functions

Configuration Effect

- Enable basic authentication and accounting services.
- On a wired network, run the **dot1x port-control auto** command in interface configuration mode to enable 802.1X authentication on a port.
- Run the **radius-server host** *ip-address* command to configure the IP address and port information of the RADIUS server and the **radius-server key** command to configure the RADIUS communication key between the NAS and the RADIUS server to ensure secure communication.

- Run the **aaa accounting update** command in global configuration mode to enable accounting update and the **aaa accounting update interval** command on the NAS to configure the accounting update interval. If the RADIUS server supports accounting update, you can also configure it on the RADIUS server. Prefer to use the parameters assigned by the authentication server than the parameters configured on the NAS.

Notes

- Configure accurate RADIUS parameters so that the basic RADIUS communication is proper.
- The 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, errors may occur during authentication and accounting.
- Due to chipset restriction on switches, if 802.1X is enabled on one port, all ports will send 802.1X packets to the CPU.
- If 802.1X is enabled on a port but the number of authenticated users exceeds the maximum number of users configured for port security, port security cannot be enabled.
- If port security and 802.1X are both enabled but the security address has aged, 802.1X users must re-initiate authentication requests to continue the communication.
- Users with IP addresses statically configured or compliant with IP-MAC binding can access the network without authentication.
- 802.1X uses the default method list by default. If the default method list is not configured for AAA, run the **dot1x authentication** and **dot1x accounting** commands to reconfigure the it.
- When SAM/SMP is used, accounting must be enabled. Otherwise, the RADIUS server will fail to detect users going offline, causing offline users remaining in the online user table.

Configuration Steps

↘ Enabling AAA

- (Mandatory) 802.1X authentication and accounting take effect only after AAA is enabled.
- Enable AAA on the NAS that needs to control user access by 802.1X.

Command	aaa new-model
Parameter Description	N/A
Defaults	AAA is disabled by default.
Command Mode	Global configuration mode
Usage Guide	AAA is disabled by default. This command is mandatory for the deployment of 802.1X authentication.

↘ Enabling an AAA Authentication Method List

- Mandatory.
- The AAA authentication method list must be consistent with the 802.1X authentication method list.

- Enable an AAA authentication method list after 802.1X authentication is enabled on the NAS.

Command	**aaa authentication dot1x** *list-name* **group radius**
Parameter Description	*list-name*: Indicates the 802.1X authentication method list of AAA.
Defaults	No AAA authentication method list is configured by default.
Command Mode	Global configuration mode
Usage Guide	AAA authentication modes are disabled by default. The AAA authentication mode must be consistent with the 802.1X authentication mode.

Configuring the RADIUS Server Parameters

- (Mandatory) The RADIUS server parameters must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure RADIUS server parameters after 802.1X authentication is enabled on the NAS.

Command	**radius-server host** *ip-address* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server. *port1*: Indicates the authentication port. *port2*: Indicates the accounting port.
Defaults	No RADIUS server parameters are configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Preshared Key for Communication between the NAS and RADIUS Server

- (Mandatory) The preshared key for communication between the NAS and RADIUS server must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure the preshared key of the RADIUS server after 802.1X authentication is enabled on the NAS.

Command	**radius-server key** *string*
Parameter Description	*string*: Indicates the preshared key.
Defaults	No preshared key is configured for communication between the NAS and RADIUS server by default.
Command Mode	Global configuration mode
Usage Guide	The IP address of the NAS must be the same as that registered on the RADIUS server. The preshared key on the NAS must be the same as that on the RADIUS server. If the default RADIUS communication ports are changed on the RADIUS server, you need to change the communication ports on the NAS correspondingly.

Enabling 802.1X on a Port

- This command is mandatory for a wired network.
- Enable 802.1X on switches.

Command	dot1x port-control auto
Parameter Description	N/A
Defaults	802.1X is disabled on a port by default.
Command Mode	Interface configuration mode, VxLAN mode
Usage Guide	802.1X is disabled on a port by default. This command is mandatory for the deployment of 802.1X authentication. The default method list is used by default. If the 802.1X authentication method list in AAA is not the default one, the configured 802.1X authentication method list should match.

Verification

Start the supplicant, enter the correct account information, and initiate authentication. Then check whether the 802.1X and RADIUS configurations are correct.

Checking for 802.1X Authentication Entries

Command	show dot1x summary
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display entries of authenticated users to check the authentication status of users, for example, authenticating, authenticated, or quiet.
Command Display	N/A

Checking for AAA User Entries

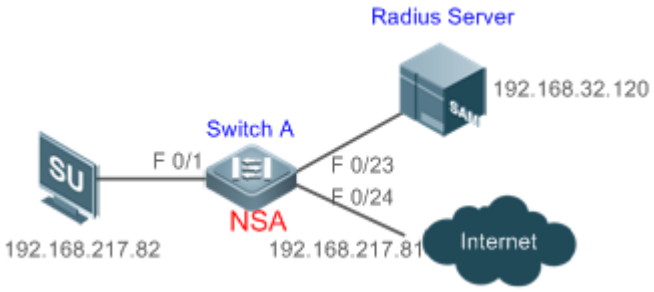
Command	show aaa user all
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display information of AAA users.
Command Display	Hostname#show aaa user all ------------------------------ Id ----- Name 2345687901 wwxy ------------------------------

- Check whether the RADIUS server responds to authentication based on the RADIUS packets between the NAS and the RADIUS server. If no, it means that the network is disconnected or parameter configurations are incorrect. If the RADIUS server directly returns a rejection reply, check the log file on the RADIUS server to identify the cause, e.g., of the authentication mode of the authentication server is incorrectly configured.

Configuration Example

In this example, SAM acts as the authentication server.

Configuring 802.1X Authentication on a Switch

Scenario **Figure 4-5**	
Configuration Steps	● Register the IP address of the switch on the RADIUS server and configure the communication key between the switch and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the switch. ● Configure RADIUS parameters on the switch. ● Enable 802.1X authentication on ports of the switch. Switch configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.

	`Hostname# configure terminal`
	`Hostname (config)# aaa new-model`
	`Hostname (config)# radius-server host 192.168.32.120`
	`Hostname (config)# radius-server key test`
	`Hostname (config)# interface FastEthernet 0/1`
	`Hostname (config-if)# dot1x port-control auto`

Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username:tests-user,password:test**. ● The user fails to ping 192.168.32.120 before authentication. ● After the user enters account information and click **Authenticate** on the supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed.

	Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --------- ---------- ---------- --------- ---- ---------- ---------- ---------- --------- ---------- 16778217 ts-user 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h 0m 7s

Common Errors

- RADIUS parameters are incorrectly configured.
- The RADIUS server has a special access policy, for example, the RADIUS packets must carry certain attributes.
- The AAA authentication mode list is different from the 802.1X authentication mode list, causing authentication failure.

4.4.2 Configuring 802.1X Parameters

Configuration Effect

- Adjust 802.1X parameter configurations based on the actual network situation. For example, if the authentication server has poor performance, you can raise the authentication server timeout.

Notes

- 802.1X and RADIUS have separate server timeouts. By default, the authentication server timeout of 802.1X is 5 seconds while that of RADIUS is 15 seconds. In actual situations, ensure that the former is greater than the latter. You can run the **dot1x timeout server-timeout** command to adjust the authentication server timeout of 802.1X. For detailed configuration about the RADIUS server timeout, see the *Configuring RADIUS*.
- Online client detection applies only to our company's supplicant.

Configuration Steps

↘ Enabling Re-authentication

- (Optional) After re-authentication is enabled, the NAS can periodically re-authenticate online users.
- Enable re-authentication after 802.1X authentication is enabled on the NAS.

Command	**dot1x re-authentication**
Parameter Description	N/A
Defaults	Re-authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	You can run this command to periodically re-authenticate users.

Configuring the Re-authentication Interval

- (Optional) You can configure the re-authentication interval for users.
- Configure the re-authentication interval after 802.1X authentication is enabled on the NAS. The re-authentication interval takes effect only after re-authentication is enabled.

Command	**dot1x timeout re-authperiod** *period*
Parameter Description	*period*: Indicates the re-authentication interval in the unit of seconds.
Defaults	The default value is 3,600 seconds.
Command Mode	Global configuration mode
Usage Guide	Adjust the re-authentication interval as required.

Configuring the Interval of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates a longer interval of packet retransmission.
- Configure the interval of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout tx-period** *period*
Parameter Description	*period*: Indicates the interval of EAP-Request/Identity packet retransmission in the unit of seconds.
Defaults	The default value is 3 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Adjust the value based on how long the authentication client responds to the NAS's requests.

Configuring the Maximum Times of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x reauth-max** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Identity packet retransmission.
Defaults	The default value is 3 for switches.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. In the case of high-rate packet loss, increase this value so that the clients can easily receive packets from the NAS.

Configuring the Interval of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates a longer retransmission interval.
- Configure the interval of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout supp-timeout** *time*
Parameter Description	*time*: Indicates the interval of EAP-Request/Challenge packet transmission in the unit of seconds.
Defaults	The default value is 3 seconds for switches.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

Configuring the Maximum Times of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x max-req** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Challenge packet retransmission in the unit of seconds.
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Optional. It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

Configuring the Authentication Server Timeout

- (Optional) A larger value indicates a longer authentication server timeout.
- Configure the authentication server timeout after 802.1X authentication is enabled on the NAS.
- The server timeout of RADIUS must be greater than that of 802.1X.

Command	**dot1x timeout server-timeout** *time*
Parameter Description	*time*: Indicates the authentication server timeout in the unit of seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value if the communication between the NAS and RADIUS server is unstable.

Configuring the Quiet Period after Authentication Fails

- (Optional) A larger value indicates a longer quiet period.
- Configure the quiet period after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout quiet-period** *time*
Parameter Description	*time*: Indicates the quiet period after authentication fails. The unit is second.
Defaults	The default value is 10 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value to prevent users from frequently initiating authentication to the RADIUS server, thereby reducing the load of the authentication server.

Specifying the Authentication Mode

- (Optional) Configure the mode for 802.1X authentication.
- Configure the authentication mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-mode** {**eap** | **chap** | **pap**}
Parameter Description	**eap**: Indicates EAP authentication. **chap**: Indicates CHAP authentication. **pap**: Indicates PAP authentication.
Defaults	The default value is **eap**.
Command Mode	Global configuration mode
Usage Guide	Select the authentication mode supported by Hostname Supplicant and authentication server.

Enabling Online Client Detection

- (Optional) If online client detection is enabled, the NAS can find clients going offline in a timely manner to prevent incorrect accounting.
- This function applies only to our company's 802.1X authentication clients.
- Enable online Hostname client detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x client-probe enable**
Parameter Description	N/A
Defaults	Online client detection is disabled by default.
Command Mode	Global configuration mode
Usage Guide	It is recommended to enable this function when the supplicant is used.

Configuring the Interval of Online Client Detection

- (Optional) A larger value indicates a longer time interval at which Hostname clients send detection packets.
- Configure the interval of online Hostname client detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x probe-timer interval** *time*
Parameter Description	*time*: Indicates the time interval at which the supplicant sends a heartbeat packet to the NAS. The unit is second.
Defaults	The default value is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value.

Configuring the Duration of Online Client Detection

- (Optional) A larger value indicates a longer interval at which the NAS finds clients going offline.
- Configure the duration of online client detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x probe-timer alive** *time*
Parameter Description	*time*: Indicates the duration of online client detection in the unit of seconds.
Defaults	The default value is 250 seconds.
Command Mode	Global configuration mode
Usage Guide	Optional. If the NAS does not receive any detection packets from an online client within the detection duration, it regards the client offline. It is recommended to use the default value.

Verification

Run the **show dot1x** command to check whether parameter configurations take effect.

Configuration Example

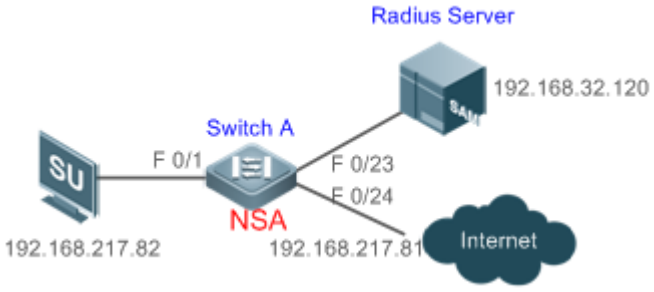
Specifying the Authentication Mode

Scenario	The NAS is deployed in standalone mode.
Configuration Steps	Set the authentication mode to **chap**.
	`Hostname(config)#dot1x auth-mode chap`

Verification	Display the configurations.
	`Hostname(config)#show dot1x`
	
	`802.1X basic information:`

```
802.1X Status ..................... enable
Authentication Mode ................ chap
Authorization mode ................. disable
Total User Number .................. 0 (exclude dynamic user)
Authenticated User Number ..... 0 (exclude dynamic user)
Dynamic User Number ................ 0
Re-authentication .................. disable
Re-authentication Period ..... 3600 seconds
Re-authentication max ..... 3 times
Quiet Period ..... 10 seconds
Tx Period ..... 30 seconds
Supplicant Timeout ..... 3 seconds
Server Timeout ..... 5 seconds
Maximum Request ..... 3 times
Client Online Probe ..... disable
Eapol Tag ..... disable
802.1x redirect ..... disable
Private supplicant only ..... disable
```

Enabling Online Client Detection

Scenario **Figure 4-6**	
Configuration Steps	Enable online client detection.
	`Hostname(config)#dot1x client-probe enable`
	● Users can remain online only when their supplicant sends online detection packets as scheduled.
Verification	● Displaythe configurations.

```
Hostname(config)#show dot1x

802.1X basic information:
  802.1X Status ..................... enable
  Authentication Mode ................ chap
  Authorization mode ................. disable
```

	Total User Number ..... 0 (exclude dynamic user) Authenticated User Number ..... 0 (exclude dynamic user) Dynamic User Number ..... 0 Re-authentication ..... disable Re-authentication Period ..... 3600 seconds Re-authentication max ..... 3 times Quiet Period ..... 10 seconds Tx Period ..... 30 seconds Supplicant Timeout ..... 3 seconds Server Timeout ..... 5 seconds Maximum Request ..... 3 times Client Online Probe ..... enable Eapol Tag ..... disable 802.1x redirect ..... disable

Common Errors

- The server timeout is shorter than the RADIUS timeout.
- Online client detection is enabled but the authentication program is not our company's supplicant.

4.4.3 Configuring Authorization

Configuration Effect

- In IP authorization, authenticated users have to use the specified IP addresses to access the network, preventing IP address fake. IP authorization can be enabled in global configuration mode or interface configuration mode. IP authorization enabled in interface configuration mode takes priority over that configured in global configuration mode.
- Enable the client filtering function. If this function is enabled, users must use our company's supplicant for authentication so that they will enjoy services provided by the supplicant, such as anti-proxy or SMS.
- Enable Web redirection to support 2G supplicant deployment. 2G supplicant deployment means that a user needs to download the supplicant through the browser and then initiate authentication through the supplicant. 2G supplicant deployment facilitates quick deployment of the supplicant in the case of massive users.

Notes

- If the real-time kickoff function of SAM/SMP is used, you need to configure correct SNMP parameters. For details, see the *Configuring SNMP*.
- If multiple authentication supplicants are used, disable this function.
- If the IP authorization mode is changed, all authenticated users will go offline and have to get re-authenticated before online again.

- In mixed authorization mode, IP authorization with a higher priority is used during user authentication. For example, if the supplicant provides an IP address for this RADIUS-authentication user during its re-authentication, this IP address will be used for authorization.
- 2G supplicant deployment and Web authentication cannot be used at the same time.
- 2G supplicant deployment requires the setting of the **redirect** parameter. For details, see the *Configuring Web Authentication*.
- The kickoff function of SAM/SMP is implemented through SNMP. Therefore, you need to configure SNMP parameters. For details, see the *Configuring SNMP*.

Configuration Steps

Specifying the Global IP Authorization Mode

- The **supplicant** mode only applies to the supplicant.
- In **radius-server** mode, the authentication server needs to assign IP addresses based on the **framed-ip** parameters.
- In **dhcp-server** mode, DHCP snooping must be enabled on the NAS.
- (Optional) Configure an IP-MAC binding.
- Configure the IP authorization mode after 802.1X authentication is enabled on the NAS.

Command	**aaa authorization ip-auth-mode** { **disable | supplicant | radius-server | dhcp-server | mixed** }
Parameter Description	**disable**: Disables IP authorization. **supplicant**: Indicates IP authorization by the supplicant. **radius-server**: Indicates IP authorization by the RADIUS server. **dhcp-server**: Indicates IP authorization by the DHCP server. **mixed**: Indicates IP authorization in a mixed manner.
Defaults	IP authorization is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Select the IP authorization mode based on actual deployment.

Enabling Web Redirection for 2G Supplicant Deployment

- (Optional) If the redirection for 2G supplicant deployment is enabled, users not having any 802.1X authentication clients on a controlled port can download and install an 802.1X authentication client through Web pages.
- Enable Web redirection for 2G supplicant deployment after 802.1X authentication is enabled on the NAS.
- The **redirect** parameter must be configured. For details, see the *Configuring Web Authentication*.

Command	**dot1x redirect**
Parameter Description	N/A
Defaults	The redirection for 2G supplicant deployment is disabled by default.

Command Mode	Global configuration mode
Usage Guide	The **redirect** parameter must be configured. For details, see the *Configuring Web Authentication*.

Enabling the Client Filtering Function

- (Optional) If this function is enabled, the clients except our company's client cannot perform authentication.
- Enable client filtering function after 802.1X authentication is enabled on the NAS.

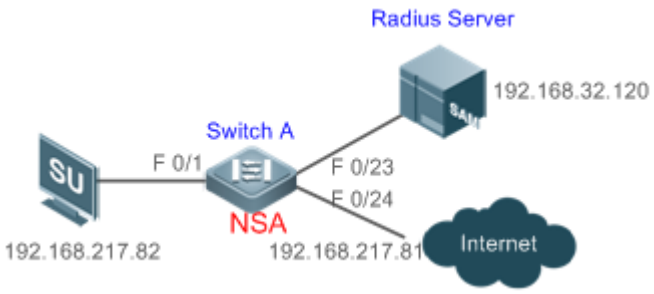
Command	**dot1x private-supplicant-only**
Parameter Description	N/A
Defaults	The client filtering function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This function can be enabled only when our company's supplicant software is used.

Verification

- After IP authorization is enabled, use the client to initiate authentication and go online, and then change the IP address. As a result, the client cannot access the network.
- Enable Web redirection for 2G supplicant deployment. When you start the browser to visit a website, the system automatically redirects to the download Web page and downloads the authentication client. You can access the network only when authenticated by the client.
- After a user is authenticated and goes online, enable the kickoff function on SAM/SMP. The NAS will force the user offline and the user will fail to access the network.

Configuration Example

Configuring the IP Authorization Mode

Scenario **Figure 4-7**	

Configuration Steps	● Enable AAA. ● Configure RADIUS. ● Enable 802.1X on a controlled port. ● Globally enable IP authorization in **supplicant** mode.
	`Hostname(config)#aaa authorization ip-auth-mode supplicant`
	● The supplicant initiates authentication and the authentication succeeds. ● The supplicant only uses 192.168.217.82 for communication.

Verification	● Display the configurations.
	`Hostname(config)#show dot1x user name ts-user`
	`Supplicant information:`
	`MAC address ..... b048.7a7f.f9f3`
	`Username ..... ts-user`
	`User ID ..... 16777303`
	`Type ..... static`
	`VLAN ..... 1`
	`Online duration ..... 0days 0h 0m21s`
	`Up average bandwidth ..... 0 kBps`
	`Down average bandwidth ..... 0 kBps`
	`Authorized VLAN ..... 1`
	`Authorized session time ..... 20736000 seconds`
	`Authorized flux ..... unlimited`
	`Accounting ..... No`
	`Proxy user ..... Permit`
	`Dial user ..... Permit`
	`IP privilege ..... 0`
	`Private supplicant ..... no`
	`Max user number on this port ..... 0`
	`Authorization ip address ..... 192.168.217.82`

Common Errors

- There are multiple authentication clients on the network but the client filtering function is enabled, causing some users to fail authentication.
- SAM/SMP is used but SNMP parameters are not configured on the switch, causing kickoff failure.
- The **redirect** parameter is incorrectly configured, causing abnormalities in redirection for 2G supplicant downloading.

4.4.4 Configuring MAB

Configuration Effect

- If the MAC address of an access user is used as the authentication account, the user does not need to install any supplicants. This applies to some dumb users such as networking printers.

- Single-user MAB applies to two scenarios:
  - There is only one dumb user connected to a port.
  - Only one user needs to be authenticated. After this, all other users can access the network.
- Multi-user MAB applies to the scenario where multiple dumb users connected to a port. For example, multiple VoIP devices are deployed in the network call center.
- Multi-user MAB can be used with 802.1X authentication. It applies to mixed access scenarios such as the PC-VoIP daisy-chain topology.

Notes

- A MAB-enabled port sends an authentication request packet as scheduled by **tx-period**. If the number of the sent packets exceeds the number specified by **reauth-max** but still no client responds, this port enters the MAB mode. Ports in MAB mode can learn the MAC addresses and use them as the account information for authentication.
- When using the MAC address as the user name and password on the authentication server, delete all delimiters. For example, if the MAC address of a user is 00-d0-f8-00-01-02, the user name and password should be set to 00d0f8000102 on the authentication server.
- 802.1X takes priority over MAB. Therefore, if a user having passed MBA authentication uses a client to initiate 802.1X authentication, MAB entries will be removed.
- MAB supports only PAP authentication. PAP authentication should be enabled also on the authentication server.
- Only when active authentication is enabled, can MAB detect whether the user can perform 802.1X authentication. Therefore, automatic authentication must be enabled for MAB deployment.

Configuration Steps

↘ Enabling Single-User MAB

- Optional.
- Single-user MAB applies when only one user connected to a port needs to be authenticated.
- Enable single-user MAB on the 802.1X controlled port of the NAS.

Command	dot1x mac-auth-bypass
Parameter Description	N/A
Defaults	Single-user MAB is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command applies only to switches. Single-user MAB applies when only one dumb user connected to a port needs to be authenticated. If you want to restrict the number of users, enable the violation mode.

↘ Configuring the Timeout of MAB Users

- Optional.

- After a MAC address in MAB mode is authenticated and goes online, the NAS regards the MAC address online unless re-authentication fails, the port goes down, or the MAC address goes offline due to management policies such as kickoff. You can configure the timeout of authenticated MAC addresses. The default value is 0, indicating always online.
- Configure the timeout of MAB users on the 802.1X controlled port of the NAS.

Command	**dot1x mac-auth-bypass timeout-activity** *value*
Parameter Description	*value*: Indicates the maximum online time of MAB users in the unit of seconds.
Defaults	The default value is 0, indicating no time restriction.
Command Mode	Interface configuration mode
Usage Guide	The MAB timeout applies to both single-user MAB and multi-user MAB.

Enabling the MAB Violation Mode

- Optional.
- Enable MAB violation on the 802.1X controlled port of the NAS.
- By default, after one MAC address passes MAB authentication, data of all switches connected to the port can be forwarded. However, for security purposes, the administrator may request one MAB port to support only one MAC address. In this case, you can enable MAB violation on the port. If more than one MAC address is found connected to a MAB violation-enabled port after the port enters MAB mode, the port will become a violation.

Command	**dot1x mac-auth-bypass violation**
Parameter Description	N/A
Defaults	MAB violation is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command applies only to switches. Configure this command only when only one dumb user is connected to the port. MAB violation applies only to single-user MAB.

Enabling Multi-user MAB

- Optional.
- Enable multi-user MAB on the 802.1X controlled port of the NAS.

Command	**dot1x mac-auth-bypass multi-user**
Parameter Description	N/A
Defaults	Multi-user MAB is disabled by default.
Command Mode	Interface configuration mode

Usage Guide	This command applies only to switches. Configure this command when multiple dumb users connected to the port need to be authenticated.

Configuring the Quiet Period after Multi-user MAB Fails

- Optional.
- Configure the quite period of the multi-user MAB failure after multi-user MAB is enabled on the NAS.
- If multi-user MAB is enabled, you should prohibit unauthorized users from frequently initiating authentication to protect the NAS from attacks of these users and thereby reduce the load of the authentication server. Configure the quite period of the multi-user MAB failure in global configuration mode. That is, if a MAC address fails authentication, it needs to re-initiate authentication after the quiet period. Configure this quiet period based on the actual situation. The default value is 0, indicating that a user can re-initiate authentication immediately after authentication fails.

Command	**dot1x multi-mab quiet-period** *value*
Parameter Description	*value*: Indicates the quiet period after authentication fails.
Defaults	The default value is 0s.
Command Mode	Global configuration mode
Usage Guide	This command applies only to switches. If too many dumb users connected to a port are authenticated, run this command to limit the authentication rate.

Configuring VLAN-based MAB

- Optional.
- Enable VLAN-based MAB after multi-user MAB is enabled on the NAS.
- If you configure VLANs as MAB VLANs, only users in these VLANs can perform MAB.

Command	**dot1x mac-auth-bypass vlan** *vlan-list*
Parameter Description	*vlan-list*: Indicates the VLANs supporting MAB.
Defaults	VLAN-based MAB is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command applies only to switches. Run this command when a port allows only users in specified VLANs to perform MAB.

Configuring the Number of Authentication Failures Required for Aging a User

- Optional.
- Configure the number after multi-user MAB is enabled on the NAS.

Command	**dot1x multi-mab quiet-user fail-times [** *fail-times* **]**

Parameter Description	*fail-times*: Sets the number of authentication failures required for aging a user. The value range is from 1 to 65,535.
Defaults	The default number of authentication failures required for aging a user is 60.
Command Mode	Global configuration mode
Usage Guide	A user who fails the authentication is required to be aged. This command is used to configure the aging rule for the user failing the authentication.

Configuring the Rate of Initiating a Blocked Multi-user MAB Entry

- Optional.
- Configure the rate after multi-user MAB is enabled on the NAS.

Command	**dot1x multi-mab quiet-user authen-num** [*authen-num*]
Parameter Description	*authen-num*: Sets the rate of initiating authentication using the MAC address in a blocked multi-user MAB user entry, in the number of MAC addresses per second. The value range is from 1 to 1000.
Defaults	50 MAC addresses per second.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Number of Server Rejections Required for Deleting a Blocked User Entry

- Optional.
- Configure the number after multi-user MAB is enabled on the NAS.

Command	**dot1x multi-mab quiet-user reject-times** [*reject-times*]
Parameter Description	*reject-times*: Sets the number of server rejections required for deleting a blocked user entry.
Defaults	The default number of server rejections required for deleting a blocked user entry is 1.
Command Mode	Global configuration mode
Usage Guide	N/A

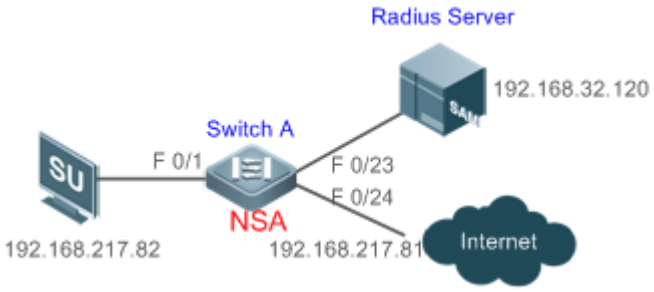
Verification

Check whether the dumb user can access the network. If yes, MAB takes effect. If no, MAB does not take effect.

- Check whether MAB functions are configured on the authentication server and NAS.
- Check whether dumb users with illegitimate MAC addresses cannot access the network.
- Check whether dumb users with illegitimate MAC addresses can access the network.

Configuration Example

Enabling Multi-user MAB on a Switch

Scenario **Figure 4-8**	
Configuration Steps	● Register the IP address of the Switch A on the RADIUS server and configure the communication key between Switch A and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on Switch A. ● Configure RADIUS parameters on Switch A. ● Enable 802.1X and multi-user MAB on a port of Switch A. Switch configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	Hostname# configure terminal Hostname (config)# aaa new-model Hostname (config)# radius-server host 192.168.32.120 Hostname (config)# radius-server key test Hostname (config)# interface FastEthernet 0/1 Hostname (config-if)# dot1x port-control auto Hostname (config-if)# dot1x mac-auth-bypass multi-user
Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username: 0023aeaa4286,password: 0023aeaa4286**. ● The user fails to ping 192.168.32.120 before authentication. ● The user connects to the switch, the authentication succeeds, and the user can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --- --- --- --- --- --- --- --- --- --- 16778217 0023aea... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h 5m 8s

4.4.5 Configuring MAB Auto Authentication

Configuration Effect

- When a STA accesses the network for the first time, Web authentication is performed. When the STA is disconnected from and then reconnects to the network, authentication is not required.

Notes

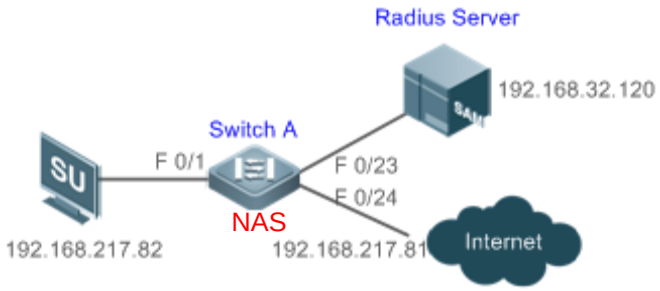
- Wireless MAB authentication is triggered by a STA advertisement. If a STA is already online, MAB authentication will not be triggered again. MAB authentication is triggered only after the STA is disconnected from and then reconnects to the network.
- When a STA accesses the network for the second time, a dialog box may be displayed for MAB authentication. When the STA accesses the network for the third time, the dialog box will not be displayed.
- If MAB authentication fails, a dialog box is displayed for Web authentication when the STA accesses the network next time.

Configuration Steps

For details about Web authentication configuration, see the Web authentication configuration document. For details about MAB authentication configuration, see section “Configuring MAB”.

Configuration Example

Configuring MAB Auto Authentication

Scenario **Figure 4-9**	
Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server and bind it with a MAC address for imperceptible authentication. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable 802.1X authentication and MAB authentication on an interface of the NAS. ● Enable second-generation (or first-generation/embedded) Web authentication on an interface of the NAS and configure the Web authentication template globally. The following describes the NAS configurations. For detailed configuration on the RADIUS server,

<table>
<tr><td></td><td>see the related configuration guide (The following describes configuration on the switch, which is similar to that on the AC/AP, except that the configuration on the switch is performed in interface configuration mode instead of WLAN RSNA configuration mode.)</td></tr>
<tr><td></td><td><pre>Hostname#configure terminal
Hostname (config)#aaa new-model
Hostname (config)#aaa authentication web-auth default group radius
Hostname (config)#aaa authentication dot1x default group radius
Hostname (config)aaa accounting net-work default start-stop group radius
Hostname (config)#radius-server host 192.168.32.120
Hostname (config)#radius-server key test
Hostname (config)#web-auth template eportalv2
Hostname (config-tmplt-v2)#ip 192.158.32.9
Hostname (config-tmplt-v2)#url http://192.168.32.9:8080/eportal/index.jsp
Hostname (config-tmplt-v2)#exit
Hostname (config)#interface FastEthernet 0/1
Hostname (config-if)#dot1x port-control auto
Hostname (config-if)#dot1x mac-auth-bypass multi-user
Hostname (config-if)#web-auth enable eportalv2</pre></td></tr>
<tr><td></td><td></td></tr>
<tr><td>Verification</td><td>Check whether authentication is normal and network access behaviors change after authentication.

The account is successfully created, for example, the username is 0023aeaa4286 and the password is 0023aeaa4286.
The STA fails to ping 192.168.32.120 before authentication.
The STA connects to the NAS, a page indicating the authentication succeeds is displayed, and the STA can successfully ping 192.168.32.120.
The STA is disconnected from and then reconnects to the network and can successfully ping 192.168.32.120.

<pre>Hostname#show dot1x summary
ID   Username   MAC   Interface VLAN Auth-State
Backend-State Port-Status User-Type Time
--------- ---------- --------------   --------- ---- ---------------
------------- ----------- --------- ------------------
16778217 0023aea... 0023.aeaa.4286 Fa0/1   2   Authenticated   Idle
Authed   static   0days 0h 5m 8s</pre></td></tr>
</table>

Common Errors

- The MAC account format is incorrect on the authentication server.

4.4.6 Configuring IAB

Configuration Effect

- Enable IAB. After IAB is enabled, newly authenticated users can access the network even when all RADIUS servers configured on the NAS are inaccessible.
- Enable IAB recovery. When RADIUS servers recover to their reachable status, re-verify the users authorized during inaccessibility.
- Configure IAB VLANs. When RADIUS servers are inaccessible and cannot authenticate users temporarily, you can add the ports connected with users to specified VLANs so that users can access only network resources of specified VLANs.

Notes

- Configure an account and standards for testing RADIUS server accessibility. For details, see the *Configuring RADIUS*.
- IAB takes effect only when only RADIUS authentication exists in the globally configured 802.1X authentication mode list and all RADIUS servers in the list are inaccessible. If other authentication modes (for example, local and none) exist in the list, IAB does not take effect.
- After multi-domain AAA is enabled, 802.1X authentication does not need the globally configured authentication mode list any more. If IAB detects that all RADIUS servers configured in the globally configured 802.1X authentication mode list are inaccessible, it directly returns an authentication success reply to users, with no need to enter the user name. Therefore, multi-domain AAA does not take effect on this port.
- Users authenticated in IAB mode do not need to initiate accounting requests to the accounting server.
- Authenticated users can properly access the network, not affected by server inaccessibility.
- In access authentication configuration mode, when 802.1X-based IP authotication is enabled globally, users on this port, except those habing been authenticated, cannot be authenticated in IAB mode. In gateway authentication mode, users are IP authorized if their IP addresses are obtained.
- Complete 802.1X authentication is required on such 802.1X authentication clients as those of Windows. It is possible that though these clients already pass the IAB authentication, there are prompts on the clients suggesting failed authentication.
- If the failed VLAN configured does not exist, a failed VLAN will be dynamically created when a port enters the failed VLAN and automatically removed when the port exits the failed VLAN.
- Failed VLANs cannot be private VLANs, remote VLANs, and super VLANs (including sub VLANs).

Configuration Steps

↘ Enabling IAB

- (Optional) After IAB is enabled, the NAS authorizes newly authenticated users if the authentication server is faulty.
- Enable IAB after 802.1X authentication is enabled on the NAS.

Command	dot1x critical

Parameter Description	N/A
Defaults	IAB is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command applies to ports on which newly authenticated users need to be authorized when the authentication server is inaccessible.

Enabling IAB Recovery

- (Optional) After the authentication server is recovered, the NAS re-authenticates users that are authorized when the authentication server is inaccessible.
- Enable IAB recovery actions after 802.1X authentication is enabled on the NAS.

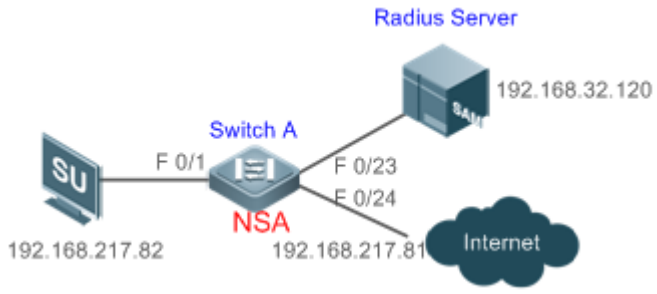
Command	**dot1x critical recovery action reinitialize**
Parameter Description	N/A
Defaults	IAB recovery is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	If IAB recovery is enabled on a port, properly authenticated users on the port can access the network without re-authentication after the authentication server is recovered. After the authentication server is recovered, the NAS initiates authentication only to users authenticated in IAB mode during server inaccessibility.

Verification

- When the authentication server is accessible, check whether users can go online only by using the correct user name and password.
- When the authentication server is inaccessible, check whether new users can be authorized to access the network immediately after connecting to the NAS.

Configuration Example

Enabling IAB

Scenario **Figure 4-10**	

Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters and enable server accessibility probe on the NAS. ● Enable 802.1X and multi-user MAB on a port of the NAS. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	Hostname# configure terminal Hostname (config)# aaa new-model Hostname (config)# radius-server host 192.168.32.120 Hostname (config)# radius-server key test Hostname (config)# interface FastEthernet 0/1 Hostname (config-if)# dot1x port-control auto
Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username: test,password: test**. ● When the authentication server is accessible, the user fails to ping 192.168.32.120 before authentication. ● When the authentication server becomes inaccessible, the user connects to the NAS, authentication succeeds, and the user can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --- --- --- --- --- --- --- --- --- --- 16778217 test 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h10m20s

4.4.7 Configuring Port Control

Configuration Effect

- By default, the 802.1X controlled port is controlled based on the MAC address. That is, users using this MAC address can access the network only after authenticated.
- Configure the port-based control mode. As long as a user on a controlled port passes authentication, this port becomes authenticated and all users connected to this port can properly access the network.
- Configure the single-user control mode on a port. This port allows only a single user to pass authentication. If this port becomes authenticated, this user can properly access the network. At this time, if the NAS detects other users connected to this port, it will clear all users connected to this port and the user needs to re-initiate authentication.

- The port-based control mode allows or prohibits dynamic users migrating among different ports. By default, dynamic users can migrate among different ports.

Notes

- In port-based authentication mode, a controlled port supports only one authenticated user while all others are dynamic users.
- In single-user port-based authentication mode, only one user on a controlled port can pass authentication and access the network. This restriction remains even when a specified number of users is configured on this port.

Configuration Steps

Enabling the MAC-based Control Mode

- (Optional) After the MAC-based control mode is enabled, each user on an 802.1X controlled port must pass MAC-based authentication to access the network.
- Enable the MAC-based control mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x port-control-mode mac-based**
Parameter Description	N/A
Defaults	The default port control mode is MAC-based control.
Command Mode	Interface configuration mode
Usage Guide	Configure the MAC-based control mode if all the users on a controlled port have to pass authentication to access the network.

Enabling the Port-based Control Mode

- (Optional) After a user on an 802.1X controlled port passes authentication, all other users on this port can access the network.
- Enable the port-based control mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x port-control-mode port-based**
Parameter Description	N/A
Defaults	The default port control mode is MAC-based control.
Command Mode	Interface configuration mode
Usage Guide	You can configure the port-based control mode if the remaining users can access the network after a user on a controlled port passes authentication.

Enabling the Single-User Port-based Control Mode

- (Optional) Configure only one dynamic user to access the network in port-based authentication mode.

- Enable the single-user port-based control mode after 802.1X authentication is enabled on the NAS.

Command	dot1x port-control-mode port-based single-host
Parameter Description	N/A
Defaults	The single-user port-based control mode is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when only the authenticated user can act as a dynamic user in port-based control mode.

Disabling Migration of Dynamic Users

- (Optional) If this function is disabled, dynamic users on a controlled port cannot migrate to other ports until the port has aged.
- Disable this function after 802.1X authentication is enabled on the NAS.

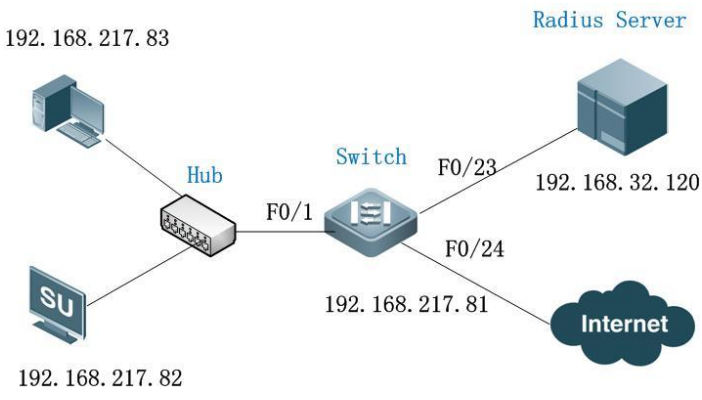
Command	dot1x stationarity enable
Parameter Description	N/A
Defaults	Dynamic users can migrate to other ports by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command to prohibit dynamic users on a controlled port from migrating to other ports.

Verification

- In MAC-based control mode, each user on a controlled port can access the network only after authenticated.
- In port-based control mode, as long as a user on a controlled port passes authentication, other users can access the network without authentication.

Configuration Example

Enabling the Port-based Control Mode

Scenario Figure 4-11	

Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable 802.1X authentication on ports of the NAS. ● Enable port-based authentication on a controlled port. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	Hostname# configure terminal Hostname (config)# aaa new-model Hostname (config)# radius-server host 192.168.32.120 Hostname (config)# radius-server key test Hostname (config)# interface FastEthernet 0/1 Hostname (config-if)# dot1x port-control auto Hostname (config-if)# dot1x port-control-mode port-based
Verification	Check whether authentication is proper, network access behaviors change after authentication, and dynamic users can access the network. ● The account is successfully created, such as **username:tests-user,password:test**. ● The user fails to ping 192.168.32.120 before authentication. ● After the user enters account information and click **Authenticate** on Hostname Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120. ● After passing authentication, dynamic users can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --------- ---------- --------------- --------- ---- --------------- ------------ ---------- --------- ------------------- 16778217 ts-user 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 2h17m29s none N/A 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed Dynamic N/A

4.4.8 Configuring Dynamic VLAN Assignment

Configuration Effect

- Enable 802.1X-based dynamic VLAN assignment for a port. If the authentication server assigns a VLAN to redirect after a user passes authentication, the NAS can add this user to the assigned VLAN to perform authorization on this user.
- Controlled ports on the VLAN to redirect fall in three types: Access, Trunk, and Hybrid (MAC VLAN is disabled). You can change native VLANs of these ports to realize 802.1X-based dynamic VLAN assignment.
- If controlled ports on the VLAN to redirect are Hybrid ports (and MAC VLAN is enabled), dynamically create MAC VLAN entries to add users to the assigned VLAN.

Notes

- The NAS can extend RADIUS attributes to assign VLANs. When assigning VLANs to the access switch based on extended attributes, the RADIUS server encapsulates these attributes in RADIUS Attribute 26, with the vendor ID of 0x00001311. The default type No. of the extended attribute is 4. You can run the **radius attribute 4 vendor-type type** command on the NAS to receive the VLAN of which the extended attribute type No. is set to **type**. For details about the command, see the *Configuring RADIUS*.
- The RADIUS server can assign VLANs based on the following RADIUS attributes:

  Attribute 64: Tunnel-Type, with the value being VLAN (13).

  Attribute 65: Tunnel-Medium-Type, with the value being 802 (6).

  Attribute 81: Tunnel-Private-Group-ID, which can be the VLAN ID or VLAN name.
- The NAS can perform 802.1X authentication on Access, Trunk, and Hybrid ports. If 802.1X-based dynamic VLAN assignment is enabled on other ports, authentication will fail.
- If the assigned VLAN is the VLAN name, the system checks whether the VLAN name exists on the access switch. If yes, the port of the user redirects to this VLAN. If no, the NAS identifies the assigned VLAN as the VLAN ID. If the VLAN ID is valid (in the VLAN ID range supported by the system), the port of the user redirects to this VLAN. If the VLAN ID is 0, no VLAN information is assigned. In other cases, users fail authentication.
- Private VLANs, remote VLANs, or super VLANs (including sub VLANs) cannot be assigned for redirection.
- In dynamic VLAN assignment on an Access port, check whether any assigned VLAN is configured on the switch:
  - Yes: If the Access port can redirect to the assigned VLAN, the port will leave the configured VLAN and migrate to the assigned VLAN, and user authentication will succeed. Otherwise (see the related description below), user authentication will fail.
  - No: If the NAS identifies the assigned VLAN attribute as the VLAN ID, it will create a VLAN and enable the port to redirect to the new VLAN, and user authentication will succeed. If the NAS identifies the assigned VLAN attribute as the VLAN name, it will fail to find the corresponding VLAN ID, causing authentication failure.
- In dynamic VLAN assignment on a Trunk port, check whether any assigned VLAN is configured on the switch:
  - Yes: If the Trunk port can redirect to the assigned VLAN, the NAS will use the native VLAN of the port as the assigned VLAN, and user authentication will succeed. Otherwise (see the related description below), user authentication will fail.
  - No: If the NAS identifies the assigned VLAN attribute as the VLAN ID, it will use the native VLAN of the port, and user authentication will succeed. If the NAS identifies the assigned VLAN attribute as the VLAN name, it will fail to find the corresponding VLAN ID, causing authentication failure.

- If MAC VLAN is disabled on a Hybrid port, check whether any assigned VLAN is configured on the switch:
  - Yes: If the Hybrid port can redirect to the assigned VLAN or the assigned VLAN does not exist in the tagged VLAN list of the Hybrid port, the NAS will allow the assigned VLAN to pass through the Hybrid port without carrying any tags and uses the native VLAN as the assigned VLAN, and user authentication will succeed. Otherwise (see the related description below), user authentication will fail.
  - No: If the NAS identifies the assigned VLAN attribute as the VLAN ID, it will create a VLAN, allow the VLAN to pass through the Hybrid port without carrying any tags, and use the native VLAN as the assigned VLAN, and user authentication will succeed. If the NAS identifies the assigned VLAN attribute as the VLAN name, it will fail to find the corresponding VLAN ID, causing authentication failure.
- If MAC VLAN is enabled on a Hybrid port, VLAN assignment is as follows:
  If the VLAN assigned by the authentication server does not exist on the NAS (MAC VLAN requires VLANs to have static configurations), or has been added to the Hybrid port with tags, or is not supported by MAC VLAN (see the *Configuring MAC VLAN*), user authentication will fail. Otherwise, the NAS will dynamically create MAC VLAN entries based on the assigned VLAN and the MAC addresses of users, and user authentication will succeed. When users go offline, MAC VLAN entries will be dynamically removed.
- If MAC VLAN is disabled on a port, VLAN assignment changes only the native VLAN but not the **native vlan** command configurations of the port. The assigned VLAN takes priority over the VLAN configured in related commands. That is, the native VLAN effective after authentication acts as the assigned VLAN while the native VLAN configured in related commands takes effect only when users go offline.
- If MAC VLAN is enabled on a port and user authentication is based on the MAC address, VLAN assignment dynamically creates MAC VLAN entries without changing the native VLAN of the port.
- No matter MAC VLAN is enabled or not on a Hybrid port, if the assigned VLAN is added to the port with tags, VLAN assignment fails.
- If MAC VLAN is enabled on a port (see the *Configuring MAC VLAN*), VLAN assignment creates an MAC VLAN entry with an all-F mask. If the MAC address of an 802.1X user is overwritten by the MAC address specified by the new MAC VLAN entry, the assigned VLAN must be the same as the VLAN specified by the new MAC VLAN entry. Otherwise, errors will occur to 802.1X users in VLAN assignment. Errors are as follows (including but not limited to): User authentication succeeds but subsequent valid data packets are discarded, causing network access failure.
  When a user goes offline by sending an EAPOL-LOGOFF packet, the 802.1X authentication entry remains on the NAS and the user status on the authentication server is still online.

Configuration Steps

Enabling Dynamic VLAN Assignment on a Port

- (Optional) After dynamic VLAN assignment is enabled on a port, authenticated users on this port will enter the assigned VLAN.
- Enable dynamic VLAN assignment after 802.1X authentication is enabled on the NAS.

Command	**dot1x dynamic-vlan enable**
Parameter	N/A

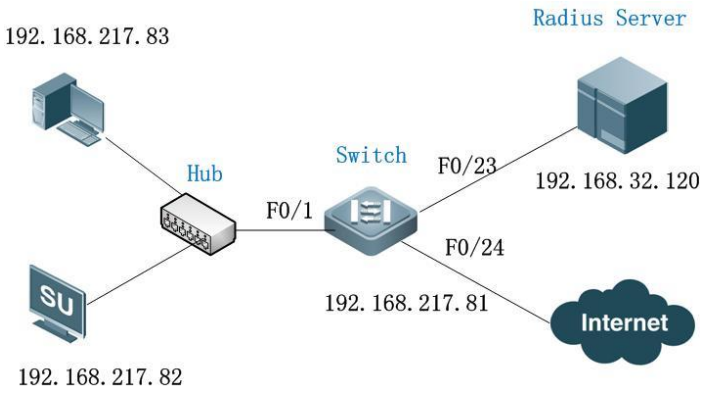
Description	
Defaults	Dynamic VLAN assignment is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when authenticated users should be added to the VLAN assigned by the authentication server.

Verification

- Run the **show dot1x summary** command to display the VLAN of a user and the **show dot1x user id** command to display the VLAN assigned by the RADIUS server.
- Users with VLANs assigned can access the network in the assigned VLANs.

Configuration Example

Enabling Dynamic VLAN Assignment on a Port

Scenario **Figure 4-12**	
Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters and enable VLAN delivery on the NAS. ● Enable 802.1X authentication on ports of the NAS. ● Enable dynamic VLAN assignment on a controlled port. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.

	`Hostname# configure terminal`
	`Hostname (config)# aaa new-model`
	`Hostname (config)# radius-server host 192.168.32.120`
	`Hostname (config)# radius-server key test`
	`Hostname (config)# interface FastEthernet 0/1`
	`Hostname (config-if)# dot1x port-control auto`

	Hostname (config-if)# dot1x dynamic-vlan enable
Verification	Check whether authentication is proper, network access behaviors change after authentication, and dynamic users can access the network. ● The account is successfully created, such as **username:tests-user,password:test**. ● The user fails to ping 192.168.32.120 before authentication. ● After the user enters account information and click **Authenticate** on the supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120. ● After passing authentication, dynamic users can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed, showing that the user jumps from VLAN 2 to VLAN 3. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --- --- --- --- --- --- --- --- --- --- 16778217 ts-user 0023.aeaa.4286 Fa0/1 3 Authenticated Idle Authed static 0days 2h17m29s

Common Errors

- RADIUS attributes for VLAN assignment are incorrectly configured on the authentication server.
- RADIUS attribute support for VLAN assignment is disabled on the NAS.
- When MAC VLAN is enabled on a Hybrid port for dynamic VLAN assignment, the assigned VLAN has tags.

4.4.9 Configuring the Guest VLAN

Configuration Effect

- If no 802.1X authentication client is available on a controlled port, add the port to the guest VLAN so that users without any authentication clients can temporarily access the network in the guest VLAN.
- If the NAS receives an EAPOL packet after adding a port to a guest VLAN, it regards that this port has an 802.1X authentication client. Then this port is forced out of the guest VLAN to perform 802.1X authentication.

Notes

- A controlled port has no 802.1X authentication client if any one of the following conditions is met:
  1. The port sends three consecutive active authentication packets but does not receive any EAPOL replies within the specified period (**auto-req req-interval** x 3).
  2. The port does not receive any EAPOL replies within 90 seconds.
  3. MAB fails.
- 802.1X-based dynamic VLAN assignment must be enabled for a port.

- When the port status switches from up to down, the port exits from the guest VLAN. When the port status switches from down to up, the NAS re-checks whether to add this port to the guest VLAN.
- If failing to receive eapol packets after 90s, an interface enters the guest VLAN. Because of the increment mechanism of sending shcp discover packets, it may take a long time for a downlink terminal to initiate a dhcp request again. Therefore, the interface cannot obtain the ip address promptly.

Configuration Steps

Configuring the Guest VLAN

- (Optional) After the guest VLAN is configured on a port, check whether the port has 802.1X authentication clients. If no, add the port to the guest VLAN.
- Configure the guest VLAN after 802.1X authentication is enabled on the NAS.

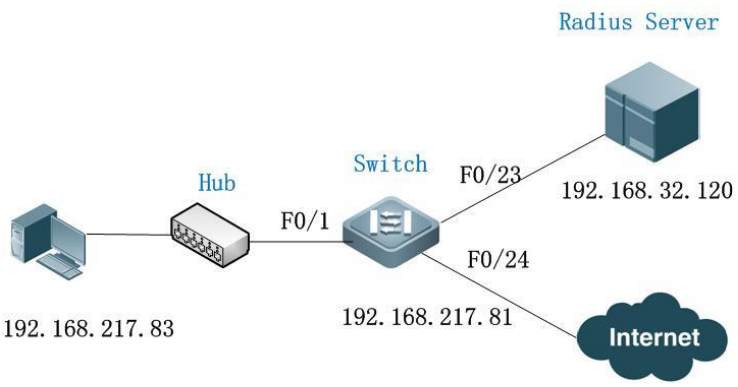
Command	**dot1x guest-vlan** *vid*
Parameter Description	*vid*: Indicates the guest VLAN to join.
Defaults	The guest VLAN is not configured by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when a user connects to an 802.1X controlled port but has no authentication client. When guest VLAN is enabled on a port, do not configure Layer-2 attributes, and specially do not manually set the VLAN of the port.

Verification

- After a port switches to the guest VLAN, users connected to the port can communicate only in the guest VLAN.
- If a user connected to a port in the guest VLAN installs an 802.1X authentication client and initiates authentication, the port will exit the guest VLAN.

Configuration Example

Configuring Dynamic VLAN Assignment and Guest VLAN

Scenario **Figure 4-13**	

Configuration Steps	● Enable 802.1X authentication on ports of the NAS. ● Enable dynamic VLAN assignment on a controlled port. ● Configure the guest VLAN on a controlled port. NAS configurations are as follows:
	Hostname (config)# interface FastEthernet 0/1 Hostname (config-if)# dot1x port-control auto Hostname (config-if)# dot1x dynamic-vlan enable Hostname (config-if)# dot1x guest-vlan 3
Verification	Check whether network access behaviors change after a port joins a guest VLAN. ● Users cannot communicate before the port joins the guest VLAN while can communicate after that. The NAS prints the log as follows: %DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface Fa0/1 from default-vlan 1 to guest-vlan 3 OK.

Common Errors

- A port receives an EAPOL packet, causing its failure to join the guest VLAN.

4.4.10 Configuring the Failed VLAN

Configuration Effect

- Configure the failed VLAN on an 802.1X controlled port. If a user fails authentication after failed VLAN is enabled, the port can be added to a failed VLAN so that the user can still access the network.
- Configure the maximum number of consecutive authentication failures. If this number is exceeded, the NAS adds the port to a failed VLAN.

Notes

- If the failed VLAN configured does not exist, a failed VLAN will be dynamically created when a port enters the failed VLAN and automatically removed when the port exits the failed VLAN.
- 802.1X-based dynamic VLAN assignment must be enabled for a port.
- If a port goes down, the port will automatically exit the failed VLAN.
- The failed VLAN and guest VLAN can be configured to the same VLAN.
- In port-based control mode, after a controlled port enters a failed VLAN, only users failing authentication can re-initiate authentication and other users' authentication requests will be discarded. This restriction does not exist in MAC-based control mode.
- Failed VLAN does not support private VLANs. That is, private VLANs cannot be configured as 802.1X failed VLANs.
- If GSN address binding is enabled on a port, users in a failed VLAN cannot access the network.

Configuration Steps

Configuring the Failed VLAN

- (Optional) If the failed VLAN is configured, the NAS adds users rejected by the authentication server to a failed VLAN.
- Configure the failed VLAN after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-fail vlan** *vid*
Parameter Description	*vid*: Indicates the failed VLAN to join.
Defaults	Failed VLAN is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command if users need to access the network even after authentication fails.

Configuring the Maximum Number of Failed VLAN Attempts

- (Optional) Configure the maximum number of times when a user is rejected by the authentication server. If this number is exceeded, the port can be added to a failed VLAN.
- Configure the maximum number of failed VLAN attempts after 802.1X authentication is enabled on the NAS.

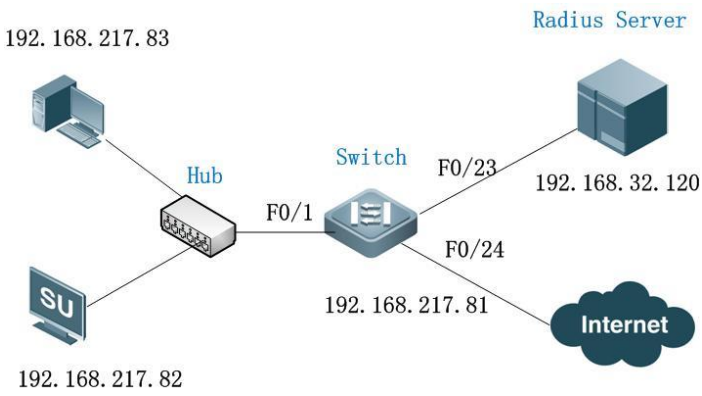
Command	**dot1x auth-fail max-attempt** *value*
Parameter Description	*value*: Indicates the maximum number of times when a user fails authentication.
Defaults	The default value is 3.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when the maximum number of failed VLAN attempts needs to be adjusted.

Verification

- When a port switches to a failed VLAN, users connected to the port can communicate only in the failed VLAN.

Configuration Example

Configuring the Failed VLAN

Scenario **Figure 4-14**	
Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable 802.1X authentication on ports of the NAS. ● Enable port-based authentication on a controlled port. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	Hostname# configure terminal Hostname (config)# aaa new-model Hostname (config)# radius-server host 192.168.32.120 Hostname (config)# radius-server key test Hostname (config)# interface FastEthernet 0/1 Hostname (config-if)# dot1x port-control auto Hostname (config-if)# dot1x auth-fail vlan 3
Verification	Check whether authentication is proper, network access behaviors change after authentication, and dynamic users can access the network. ● The account is successfully created, such as **username:tests-user,password:test**. ● The user fails to ping 192.168.32.120 before authentication. ● Start the supplicant, enter incorrect account information, and click **Authenticate**. The authentication fails, the user can successfully ping the IP address of a failed VLAN. ● Information of the authenticated user is displayed. Hostname(config)#show dot1x user name ts-user Supplicant information: MAC address ..... b048.7a7f.f9f3 Username ..... ts-user User ID ..... 16777303 Type ..... static

```
VLAN ................................ 1
Port ................................ wlan 1
Online duration ..................... 0days 0h 0m21s
Up average bandwidth ................ 0 kBps
Down average bandwidth .............. 0 kBps
Authorized VLAN ..................... 1
Authorized session time ............. 20736000 seconds
Authorized flux ..................... unlimited
Accounting .......................... No
Proxy user .......................... Permit
Dial user ........................... Permit
IP privilege ........................ 0
Private supplicant .................. no
Authorized by Auth-Fail-Vlan ........ 3
Max user number on this port ........ 0
```

Common Errors

- If a user fails authentication not due to rejection of the authentication server, for example, due to installation failure as a result of hardware resource insufficiency, it cannot enter the failed VLAN.

4.4.11 Configuring Extended Functions

Configuration Effect

- Some users use authentication clients embedded in the operating system. These clients may not initiate authentication immediately after the users access the network, affecting user experience on network access. Enable active authentication to so that such users can initiate authentication immediately after accessing the network.
- Active authentication means that the NAS sends a request/id packet to trigger the supplicant to perform 802.1 authentication. Therefore, you can use this function to detect whether the supplicant is used. For example, this function is required for MAB deployment.
- Configure the authenticable host list to specify users that can be authenticated on the port, which restricts physical access points of users to enhance network security
- The multi-account function allows a user to switch its account upon re-authentication. In special scenarios such as Windows domain authentication, multiple authentications are required to access the domain and the user account changes during authentication. This function applies to these scenarios.
- By default, the NAS uses its own MAC address as the source MAC address of EAP packets during 802.1X authentication. Some versions of the supplicants check whether the access switch is a switch based on the MAC address of EAP packets and implement some private features. When performing 802.1X authentication with these supplicants, you can enable the virtual source MAC address to use related private features.

- 802.1X allows users to obtain IP addresses before accounting. In this manner, the IP address is carried during user accounting, meeting service requirements. After a user is authenticated and goes online, the NAS can obtain the IP address of the user from the supplicant or through DHCP snooping, and then 802.1X server initiates an accounting request. To avoid the case in which the NAS does not initiate accounting for a long time due to failure to obtain the IP address of the authentication client, configure the IP detection timeout for this function. If the NAS does not obtain the IP address of the user within the configured time (5 minutes by default), it forces the user offline.
- If 802.1X authentication and MAB are enabled, you can specify the priorities of 802.1X authentication and MAB on the same port. By default, the one triggered first should be first performed and 802.1X authentication takes priority over MAB. That is, if the NAS receives an EAPOL packet from a user after the user performs MAB, the original MAB user goes offline and performs 802.1X authentication. At present, you can configure each user to first perform 802.1X authentication. If a user performs MAB following the 802.1X authentication failure and MAB takes priority over 802.1X authentication, the user can ignore 802.1X authentication after passing MAB.When 802.1X authentication is performed for an H3C inode client on a switch, the user name provided by the client for authentication is in an unrecognized format. As a result, the authentication fails. In addition, the H3C authentication server requires the user name to be in xx-xx-xx-xx-xx-xx format for MAB authentication, which is different from the default MAB authentication user name format xxxxxxxxxxxx of devices. As a result, the authentication fails.A command needs to be provided to control the 802.1X authentication user name and MAB authentication user name to be compatible with this scenario.
- 802.1X authentication can be enabled or disabled globally. If 802.1X authentication is globally disabled, users can access the internet without authentication while authenticated users are not affected. When 802.1 authentication is globally enabled, users have to pass authentication to access the internet.

Notes

- The multi-account function must be disabled if accounting is enabled. Otherwise, accounting may be inaccurate.
- MAB requires active authentication. Therefore, active authentication must be enabled if MAB is enabled.
- IP-based accounting is not required in two situations:
  - IPv4 addresses and the supplicant are deployed. This function is not required because the supplicant can upload the IPv4 addresses of users.
  - Static IP addresses are deployed.

Configuration Steps

↘ Enabling Active Authentication

- (Optional) If active authentication is enabled, the controlled port sends an authentication request actively after configuration. After receiving this request, the authentication client initiates 802.1X authentication.
- Enable active authentication after 802.1X authentication is enabled on the NAS.

Command	dot1x auto-req
Parameter Description	N/A
Defaults	Apart from on N1800K switches, active authentication is enabled by default.
Command	Global configuration mode

Mode	
Usage Guide	The destination addresses of active authentication packets are the multicast address. If the connected clients may not initiate authentication automatically, configure this command to make the NAS actively initiate authentication. When controlled ports are Trunk ports, enable active authentication so that authentication requests can be sent based on each VLAN of trunk ports.

Configuring the Number of Active Authentication Requests

- (Optional) Configure the number of active authentication requests sent by the NAS.
- Configure the number of active authentication requests after 802.1X authentication is enabled on the NAS.

Command	**dot1x auto-req packet-num** *num*
Parameter Description	*num*: Indicates the number of active authentication requests.
Defaults	The number of active authentication request is not configured by default.
Command Mode	Global configuration mode
Usage Guide	If active authentication is enabled, configure this command to restrict the number of active authentication packets sent by a port and thereby avoid sending excessive packets.

Enabling User Detection for Active Authentication

- (Optional) Configure the NAS not to send authentication requests actively if there are authenticated users on a controlled port.
- Enable user detection for active authentication after 802.1X authentication is enabled on the NAS.

Command	**dot1x auto-req user-detect**
Parameter Description	N/A
Defaults	User detection for active authentication is enabled by default.
Command Mode	Global configuration mode
Usage Guide	After this command is configured, the NAS does not send authentication packets actively if there are authenticated users on controlled Access ports. On Trunk ports, the NAS checks for authenticated users based each VLAN. If there are authenticated users on a VLAN, the NAS does not send authentication packets automatically.

Configuring the Interval of Active Authentication Request

- (Optional) Configure the interval at which the NAS sends an authentication request actively.
- Enable the interval of active authentication request after 802.1X authentication is enabled on the NAS.

Command	**dot1x auto-req req-interval** *time*

Parameter Description	*Time*: Indicates the interval of active authentication request.
Defaults	The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Authenticatable Client List

- (Optional) Configure the authenticable client list on a controlled port. Only clients on the list can perform 802.1X authentication.
- Configure the authenticable client list after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-address-table address** *mac-addr* **interface** *interface*
Parameter Description	*mac-addr*: Indicates the MAC address of the access user. *interface*: Indicates the port of the access user.
Defaults	All users can perform authentication.
Command Mode	Global configuration mode
Usage Guide	Configure this command when specified users should be able to perform authentication on a controlled port.

Enabling 802.1X Packets Sending with the Pseudo Source MAC Address

- (Optional) Configure the **dot1x pseudo source-mac** command when our company's supplicant fails to identify the NAS as our company's device based on the MAC address of the NAS.
- Configure the pseudo MAC address as the source MAC address for 802.1X authentication after 802.1X authentication is enabled on the NAS.

Command	**dot1x pseudo source-mac**
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when some of our company's supplicants cannot identify the NAS as our company's device based on the source MAC address in the EAPOL packet sent by the NAS or implement private attributes during authentication. If this command is configured, the EAPOL packet sent by the NAS uses 00-1A-A9-17-FF-FF as the source MAC address so that these supplicants can identify the NAS as our company's device.

Enabling Multi-account Authentication with One MAC Address

- (Optional) Run the **dot1x multi-account enable** command to allow the same MAC address to be used by multiple accounts.

- Enable multi-account authentication with one MAC address after 802.1X authentication is enabled on the NAS.

Command	**dot1x multi-account enable**
Parameter Description	N/A
Defaults	Multi-account authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when multi-account authentication is required in 802.1X authentication, e.g. in the case of Windows domain authentication. In this case, the authentication client can directly use a new account to initiate authentication while the previous account is still online. Multi-account authentication is disabled by default.

Configuring the Maximum Number of Authenticated Users on a Port

- (Optional) You can restrict the number of online users on a controlled port, including static users and dynamic users.
- Configure the maximum number of authenticated users on a port after 802.1X authentication is enabled on the NAS.

Command	**dot1x default-user-limit** *num*
Parameter Description	*num*: Indicates the maximum number of online users.
Defaults	There is no restriction on the number of users on a port by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when there is a need to restrict the number of authenticated users on a port.

Enabling IP-triggered Accounting

- (Optional) If IP-triggered accounting is enabled, the NAS sends an accounting request to the authentication server after obtaining the IP address of the user.
- Enable IP-triggered accounting after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct enable**
Parameter Description	N/A
Defaults	IP-triggered accounting is disabled by default.
Command Mode	Global configuration mode
Usage Guide	If both accounting and IP-triggered accounting are enabled, the NAS initiates accounting only after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address. If accounting is disabled but IP-triggered accounting is enabled, the NAS does not initiate accounting after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address within the timeout.

Configuring the Timeout of Obtaining IP Addresses After Authentication

- (Optional) Configure the timeout of obtaining IP addresses if IP-triggered accounting is enabled.
- Configure the IP address obtaining timeout after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct timeout** *time*
Parameter Description	*time:* Indicates the timeout in the unit of minutes.
Defaults	The default value is 5 minutes.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Configure this command when there is a need to change the IP address obtaining timeout after users pass authentication.

Enabling 802.1X Precedence over MAB

- (Optional) If 802.1X precedence over MAB is enabled, a user first performs 802.1X authentication. If 802.1X authentication fails, the user initiates MAB and MAB takes priority of 802.1 authentication.
- 802.1X authentication and MAB must be enabled on a port.

Command	**dot1x auth-with-order**
Parameter Description	N/A
Defaults	802.1X precedence over MAB is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	Configure this command when a user needs to first perform 802.1X authentication and initiate MAB if 802.1X authentication fails, and MAB takes priority of 802.1 authentication.

Configuring the Compatibility Function for H3C 802.1X Authentication Clients and Authentication Servers

- (Optional) This function is effective to 802.1X-authenticated and MAB-authenticated users.

Command	**dot1x user-name compatible**
Parameter Description	-
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enable this function when the H3C authentication client and authentication server are used for 802.1X authentication or the H3C authentication server is used for MAB authentication.

Disabling Global 802.1X

- (Optional) This function is effective to both 802.1x and MAB-authenticated users.

Command	**dot1x system disable**
Parameter	-

Description	
Defaults	By default, global 802.1x is enabled.
Command Mode	Global configuration mode
Usage Guide	When the server is unreachable, disable global 802.1x, so users can access the Internet without authentication. After the server resumes reachability, enable global 802.1x, and users have to pass authentication before accessing the Internet.

Enabling the Compatibility with Third-Party Supplicants

- Optional.

Command	**dot1x not-private-supplicant compatible**
Parameter Description	N/A
Defaults	By default, the device is not compatible with third-party supplicants.
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, the device can receive TLV-encoded reply msg packets sent by third-party supplicants. In the packets, the type field is of 1 byte and has a fixed value of 09; the length field occupies 1 byte; the value field refers to the character string.

4.5 Monitoring

Clearing

Authentication user information can be cleared after 802.1X is disabled.

Description	Command
Clears 802.1X user information.	**no do1x port-control auto**
Clears 802.1X user information.	**clear dot1x user**
Restores the default 802.1X configuration.	**dot1x default**

Notes

- The **dot1x default** command is used to restore global configurations.

Description	Command
Restore the default value of status machine timeout duration.	**dot1x timeout quiet-period** **dot1x timeout server-timeout** **dot1x timeout supp-timeout** **dot1x timeout tx-period**

Restore default values of configurations related to re-authentication.	**dot1x re-authentication** **dot1x timeout re-authperiod** **dot1x reauth-max**
Restore default values of configurations related to proactive requests.	**dot1x auto-req** **dot1x auto-req user-detect** **dot1x auto-req req-interval** **dot1x auto-req packet-num**
Restores the default value of the number of retransmission times.	**dot1x mac-req**
Restores the default value of the authentication mode.	**dot1x auth-mode**
Restore the default values of configurations related to client probing.	**dot1x client-probe enable** **dot1x probe-timer alive** **dot1x probe-timer interval**
Restores the default value of the function of supporting only the private client.	**dot1x private-supplicant-only**
Restores the default value of the pseudo source MAC address function.	**dot1x pseudo source-mac**
Restores the default value of the number of VLAN redirection times upon authentication failures.	**dot1x auth-fail max-attempt**
Restores the default value of the function of one MAC address for multiple accounts.	**dot1x multiaccount enable**
Restores the default value of the dot1x redirection function.	**dot1x redirect**
Restores the default value of the silent timeout duration.	**dot1x multi-mab quiet-period**
Restore the default values of functions related to accounting after obtaining the IP address.	**dot1x valid-ip-acct enable** **dot1x valid-ip-acct timeout**

Displaying

Description	Command
Displays the parameters and status of the RADIUS server.	**show radius server**
Displays 802.1X status and parameters.	**show dot1x**
Displays the authenticable host list.	**show dot1x auth-address-table**

Displays the active authentication status.	**show dot1x auto-req**
Displays the port control status.	**show dot1x port-control**
Displays the status and parameters of host probe.	**show dot1x probe-timer**
Displays of the information of authenticated users.	**show dot1x summary**
Displays the maximum times of EAP-Request/Challenge packet retransmission.	**show dot1x max-req**
Displays the information of controlled ports.	**show dot1x port-control**
Displays the client filtering information.	**show dot1x private-supplicant-only**
Displays the re-authentication status.	**show dot1x re-authentication**
Displays the maximum times of EAP-Request/Identity packet retransmission.	**show dot1x reauth-max**
Displays the quiet period after authentication fails.	**show dot1x timeout quiet-period**
Displays the re-authentication interval.	**show dot1x timeout re-authperiod**
Displays the authentication server timeout.	**show dot1x timeout server-timeou**t
Displays the supplicant timeout.	**show dot1x timeout supptimeout**
Displays the interval of EAP-Request/Identity packet retransmission.	**show dot1x timeout tx-period**
Displays user information based on the user ID.	**show dot1x user id**
Displays user information based on the MAC address.	**show dot1x user mac**
Displays user information based on the user name.	**show dot1x user name**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs AAA. (For details, see the	**debug aaa**

Configuring AAA.)	
Debugs RADIUS. (For details, see the *Configuring RADIUS*.)	**debug radius**
Debugs 802.1X events.	**debug dot1x event**
Debugs 802.1X packets.	**debug dot1x packet**
Debugs 802.1X state machine (STM).	**debug dot1x stm**
Debugs 802.1X internal communication.	**debug dot1x com**
Debugs 802.1X errors.	**debug dot1x error**

5 Configuring Web Authentication

5.1 Overview

5.1.1 Web Authentication

Web authentication controls user access to networks. It requires no authentication software on clients. Instead, users can perform authentication on common browsers.

When unauthenticated clients attempt to access the Internet using browsers, the network access server (NAS) forcibly redirects the browsers to a specified site pointing to a Web authentication server, also called a portal server. Users can access the services on the portal server before being authenticated, such as downloading security patches and reading notices. If a user wants to access network resources beyond the portal server, the user must get authenticated by the portal server through a browser.

Besides providing convenient authentication, the portal server performs Webpage interaction with browsers, providing personalized services, such as advertisements, notices, and business links on the authentication page.

Web Authentication Versions

There are three versions of Web authentication, including First-Generation Web Authentication and Second-Generation Web Authentication. The Web authentication process varies with authentication versions. For details, see Section 5.3 Features.

- The three versions of Web authentication are highly divergent in features and configurations. It is recommended to read through the relevant chapters carefully before configuration.
- Second-Generation Web Authentication supports local account authentication on the NAS. Because Remote Authentication Dial In User Service (RADIUS) authentication is more commonly used in reality, it is used as an example in the chapter "Applications".
- The concept of "interface" varies with product types. For example, the interfaces on a layer-2 switch are physical ports. This document uses the unified term "interface" to include them. In application, recognize the real meaning based on specific products and functions.
- Web authentication supports user online traffic detection. For details, see the Configuring SCC.
- 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 the Configuring AAA.
- The performance of web authentication is poor on medium and low-end devices (such as an S2915-L and other single-core devices). When the background traffic is relatively complex, the terminal service does not recognize that the switch is still sending HTTP packets continuously after restart. The terminal services occupy the insufficient bandwidth resource by which the medium and low-end devices send HTTP packets to the CPU. (These packets are forwarded by hardware before restart and do not occupy the CPU resource.). The invalid HTTP packets sent to the CPU increases

CPU usage and reduces the efficiency of Web authentication. HTTP requests for common authentication fail to obtain an effective response. The problem can be observed from slow web authentication and high CPU usage.

The following only introduces Web Authentication.

Protocols and Standards

- HTTP: RFC1945 and RFC2068
- HTTPS: RFC2818
- SNMP: RFC1157 and RFC 2578
- RADIUS: RFC2865, RFC2866, and RFC3576

5.2 Applications

Application	Description
Basic Scenario of Web Authentication	Basic layer-2 authentication scenario, where a NAS, portal server, and RADIUS server constitute an authentication system which connects a client with the NAS through the layer-2 network.

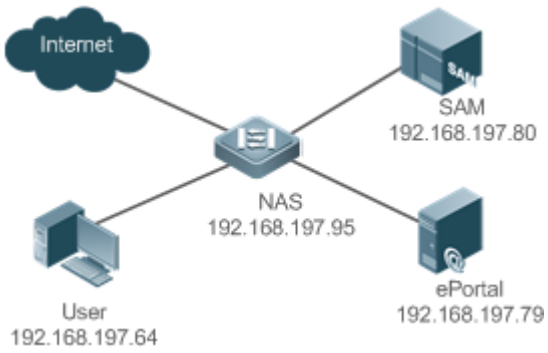
5.2.1 Basic Scenario of Web Authentication

Scenario

See Figure 5-1.

- Deploy a Web authentication scheme on the NAS.
- The client connected to the NAS needs to pass Web authentication before accessing the Internet.

Figure 5-1 Networking Topology of Web Authentication



Remarks	Web authentication is applicable to both layer-2 and layer-3 networks. At layer 3, the source MAC address and VID of a packet are changed after it is routed, but the source IP address remains the same as the only identifier of a client. Therefore, the binding policy of Web authentication on layer-3 devices must adopt the IP-only binding mode. Here, layer-2 NAS is used as an example. SAM program is installed on the RADIUS server. ePortal program is installed on the portal server.

Deployment

- Enable Web authentication on the client-accessed interface or globally on the NAS (globally on EG devices).
- Configure the ePortal server and the communication key on the NAS (for only First-Generation and Second-Generation Web Authentication).
- Configure the Simple Network Management Protocol (SNMP) communication parameters of the ePortal server on the NAS (for only First-Generation and Second-Generation Web Authentication).
- Configure the consistent communication parameters on the ePortal server and SAM server (for only First-Generation Web Authentication).
- Create user accounts on the SAM server.
- Configure AAA and method lists on the NAS (for only Second-Generation Web Authentication).
- Configure the IP address of the SAM server on the NAS (for only Second-Generation Web Authentication).
- Configure the names of the Web authentication method lists on the NAS (for only Second-Generation Web Authentication).

5.3 Features

Basic Concepts

First-Generation Web Authentication

First-Generation Web Authentication should cooperate with the ePortal software. The server installed with ePortal provides a login page to submit user authentication information, and initiates an authentication request to the RADIUS server directly. After authentication succeeds, the NAS gets user information delivered through the SNMP protocol, and thereby controls user access permissions. Communication during Web authentication of this version depends on private SNMP nodes. Moreover, the ePortal server takes the place of the NAS in authentication and accounting, which relieves the NAS from service burden.

Second-Generation Web Authentication

Second-Generation Web Authentication complies with the *CMCC WLAN Service Portal Specification*. The portal server is responsible only for Webpage interaction with users. The NAS interacts with the RADIUS server to implement authentication. The interaction between the portal server and the NAS complies with the *CMCC WLAN Service Portal Specification*. The portal server provides a login page for users to submit their information, and informs the NAS of user information through the portal protocols. The NAS completes authentication by interacting with the RADIUS server based on the user information, assigns access permissions to authenticated clients, and returns authentication results to the portal server.

The implementation process of Second-Generation Web Authentication is mainly completed on the NAS. This raises a higher demand on the NAS's capability to handle heavy tasks. Meanwhile, the portal server is simplified. The standard *CMCC WLAN Service Portal Specification*, which gains highly industry support, enables various vendors to develop compatible products.

Version Comparison

Authentication roles:

- Client: Its functions are the same among the three types of Web authentication.
- NAS: In First-Generation Web Authentication, the NAS implements only URL redirection and exchanges user login/logout notifications with the portal server. In Second-Generation Web Authentication, the NAS is responsible for redirecting and authenticating users as well as notifying the portal server of authentication results.
- Portal server: In First-Generation Web Authentication, the portal server is responsible for interaction with clients through Webpages, authenticating users, and notifying the NAS of authentication results. In Second-Generation Web Authentication, the portal server is responsible for interacting with clients through Webpages, notifying the NAS of users' authentication information, and receiving authentication results from the NAS.
- RADIUS server: Its functions are the same among the three types of Web authentication.

Authentication process:

- In Second-Generation Web Authentication, the authentication and accounting functions are transferred from the portal server to the NAS.
- Because authentication proceeds on the NAS, the second-generation NAS does not need to wait for the authentication results notified by the portal server as the first generation.

Logout process:

- In First-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, or traffic detection or port status detection performed by the NAS. In Second-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS.
- In First-Generation Web Authentication, Accounting Stop packets are sent by the portal server. In Second-Generation Web Authentication, Accounting Stop packets are sent by the NAS.

The selection of the Web authentication versions depends on the type of the portal server in use.

Command parameters in this document may be shared by the three Web authentication versions or not. Read through this document carefully to avoid parameter misconfiguration that will affect Web authentication.

Overview

Feature	Description
First-Generation Web Authentication	The portal server is deployed and supports only First-Generation Web Authentication.
Second-Generation Web Authentication	The portal server is deployed and complies with the *CMCC WLAN Service Portal Specification*.

5.3.1 First-Generation Web Authentication

HTTP Interception

HTTP interception means the NAS intercepts to-be-forwarded HTTP packets. Such HTTP packets are initiated by the browsers of the clients connected to the NAS, but they are not destined for the NAS. For example, when a client attempts to visit the website www.google.com using the Internet Explorer, the NAS is expected to forward the HTTP request packets to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

After HTTP interception is successful, the NAS redirects the HTTP requests from the client to itself to establish a session between them. Then, the NAS pushes a Webpage to the client through HTTP redirection, which can be used for authentication, software downloading or other purposes.

You can specify the clients and destination interfaces to enable or disable HTTP interception for Web authentication. In general, HTTP requests from unauthenticated clients will be intercepted, and those from authenticated clients will not. HTTP interception is the foundation of Web authentication. Web authentication is automatically triggered once HTTP interception succeeds.

HTTP Redirection

According to HTTP protocols, after the NAS receives a HTTP GET or HEAD request packet from a client, a packet with 200 (Ok) status code is replied if it is able to provide the required resources, or a packet with 302 (Moved Temporarily) status code is returned if unable. Another URL is provided in the 302 packet. After receiving the packet, the client may resend a HTTP GET or HEAD request packet to the new URL for requesting resources. This process is called redirection.

HTTP redirection is an important procedure following HTTP interception in Web authentication. It takes the advantage of 302 status code defined in HTTP protocols. HTTP interception creates a session between the NAS and a client. The client sends HTTP GET or HEAD request packets (which should have been sent to another site) to the NAS. The NAS responds with a 302 packet with a specific redirection page. Thereby, the client resends the requests to the redirection page.

Because more and more application programs run HTTP protocols, the use of the 302 redirection packet may divert a large amount of HTTP traffic (not sent by browsers) to the portal server, which will affect network authentication. To address this problem, HTTP redirection technology on the NAS adopts noise reduction to replace the 302 packets with the **js** script.

Working Principle

Figure 5-1 shows the networking topology of Web authentication.

First-generation Webauth roles:

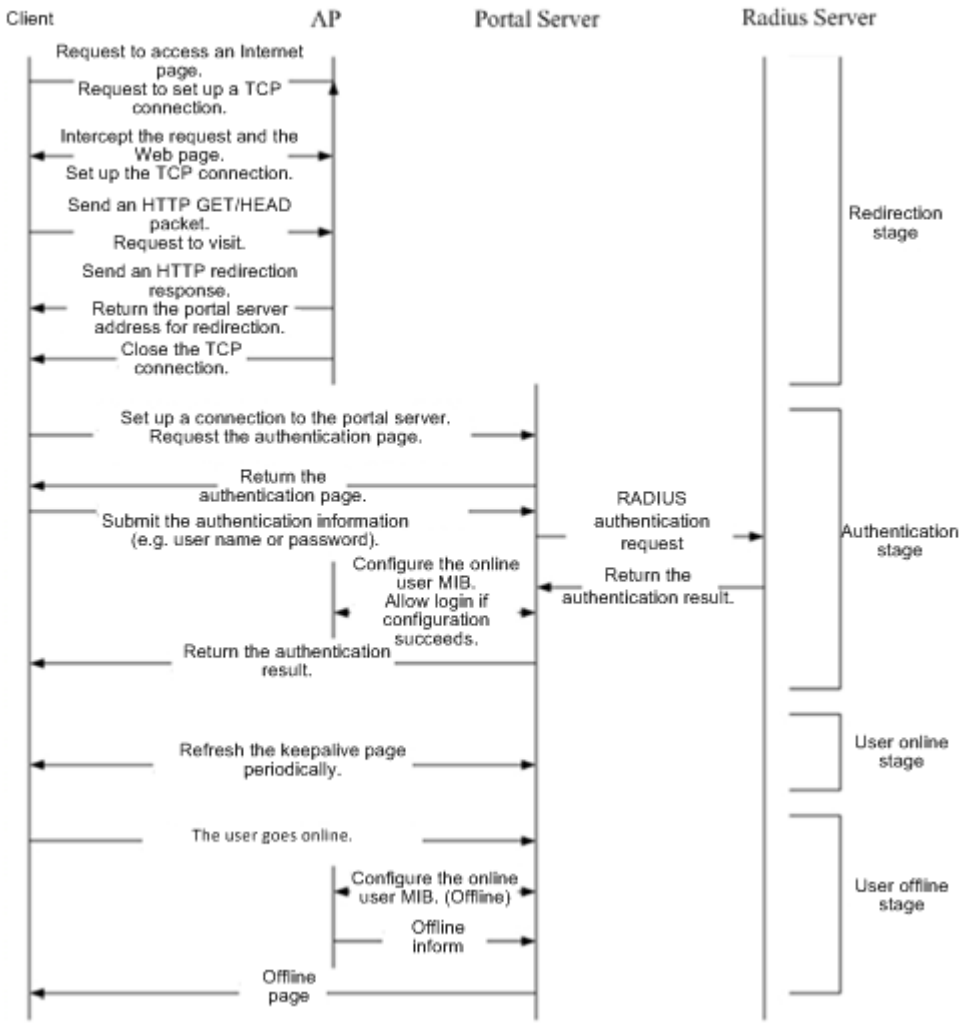
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network. The NAS is directly connected to clients and must be enabled with Web authentication.
3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, sends the information to the RADIUS server for authentication, and notifies the client and NAS of the authentication result. Figure 5-1 shows our company's ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. The portal server extracts users' authentication account information from HTTP packets and initiates authentication requests to the RADIUS server through the RADIUS protocol. The RADIUS server returns the authentication result to the portal server through the RADIUS protocol. Figure 5-1 shows the RADIUS server installed with the SAM program.

First-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server and complete authentication.
3. After the user is authenticated, the portal server notifies the NAS that the client has passed authentication, and the NAS allows the client to access resources on the Internet.

Figure 5-2 shows the flowchart of First-Generation Web Authentication by using an AP as the NAS.

Figure 5-2 Flowchart of First-Generation Web Authentication



First-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. Scenario 1: The NAS detects a client to logout and informs the portal server. Then the portal server deletes the user information on the NAS through SNMP and displays a logout page to the client.
2. Scenario 2: The portal server detects a client to logout and informs the NAS through SNMP and displays a logout page to the client.
3. In the two scenarios, the portal server sends an Accounting Stop request to the RADIUS server and notifies the RADIUS server that the client has logged out.

Related Configuration

Configuring the First-Generation Webauth Template

By default, the first-generation Webauth template is not configured.

Run the **web-auth template eportalv1** command in global configuration mode to create the first-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address*} command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string*} command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** {*string*} command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling First-Generation Web Authentication

By default, First-Generation Web Authentication is disabled.

Run the **web-auth enable{eportalv2 |** *template-name* **v2}** command in interface configuration mode to enable First-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Configuring the SNMP-Server Host

By default, the SNMP-server host and community string are not configured.

Run the **snmp-server host** {*ip-address* }**version 2c** {*community-string* }**web-auth** command in global configuration mode to configure the SNMP-server host and community string for Web authentication.

The SNMP-server host is configured to receive Inform/Trap packets of user logout.

Configuring the SNMP-Server Community String

By default, the SNMP-server community string is not configured.

Run the **snmp-server community** {*community-string*} **rw** command in global configuration mode to configure the SNMP-server community string.

The SNMP-server community string is configured to read/write user information from/to the NAS.

Enabling the SNMP Trap/Inform Function

By default, the SNMP Trap/Inform function is disabled.

Run the **snmp-server enable traps web-auth** command in global configuration mode to enable the SNMP Trap/Inform function.

The SNMP Trap/Inform function is configured to enable the NAS to inform the portal server of user logout.

5.3.2 Second-Generation Web Authentication

HTTP Interception

Same as the HTTP interception technology of First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of First-Generation Web Authentication.

Working Principle

Figure 5-1 shows the networking topology of Web authentication.

Second-generation Webauth roles:

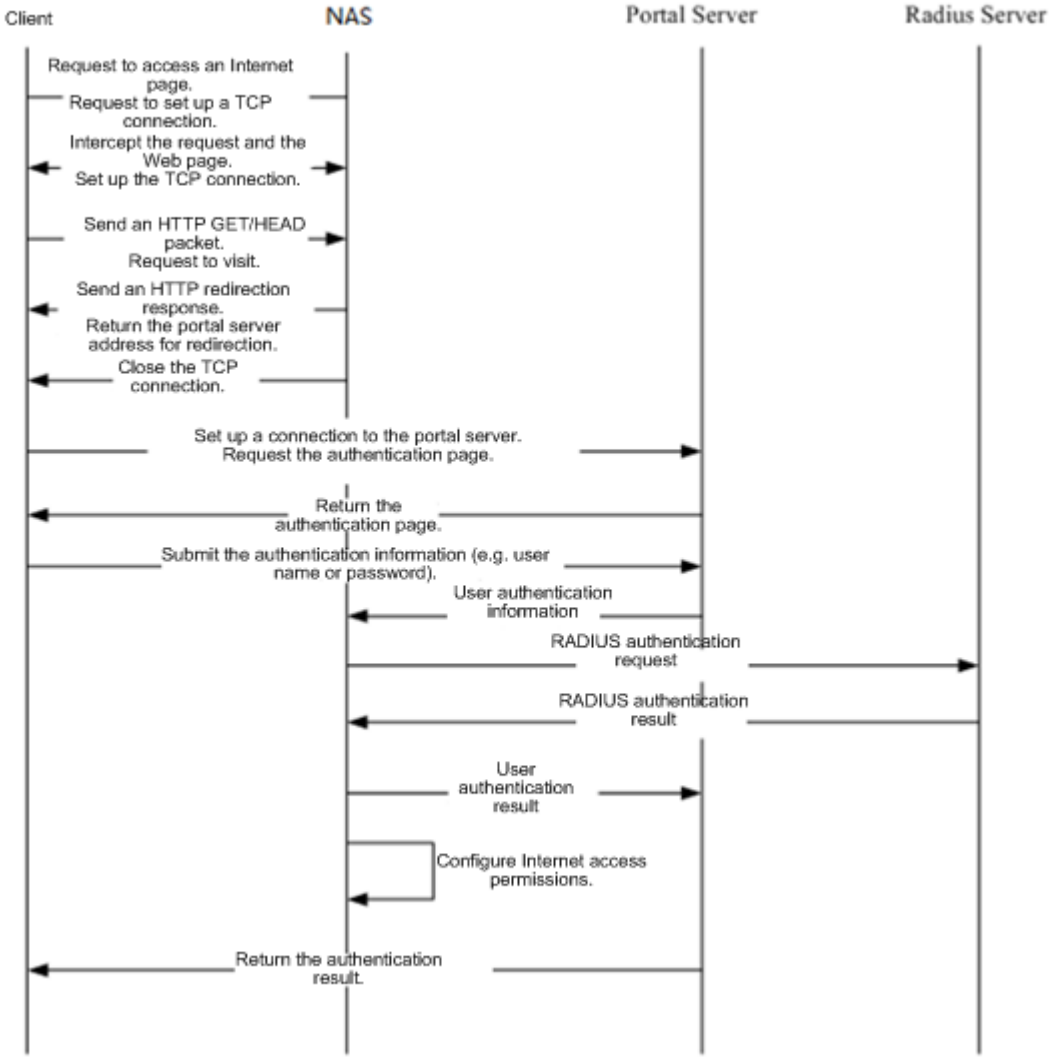
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network. The NAS is directly connected to clients and must be enabled with Web authentication. The NAS receives user authentication information from the portal server, sends authentication requests to the RADIUS server, determines whether users can access the Internet according to authentication results, and returns the authentication results to the portal server.

3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, transfers the information to the NAS, and displays the authentication result returned by the NAS to the user on a page. Figure 5-1 shows our company's ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 5-1 shows the RADIUS server installed with the SAM program.

Second-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.
3. The portal server sends the user authentication information to the NAS.
4. The NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.
5. The portal server displays the authentication result (success or failure) to the user on a page.

Figure 5-3 Flowchart of Second-Generation Web Authentication



Second-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. When a user clicks the **Logout** button on the online page, the portal server notifies the NAS to get the user offline.
2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.
3. When the RADIUS server plans to force a client offline based on a certain policy, the NAS notifies the portal server to push a logout page to the client.

Related Configuration

↘ **Configuring the Second-Generation Webauth Template**

By default, the second-generation Webauth template is not configured.

Run the **web-auth template{eportalv2 |** *template-name* **v2}** command in global configuration mode to create a second-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** { *string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling Second-Generation Web Authentication

By default, Second-Generation Web Authentication is disabled.

Run the **web-auth enable {eportalv2 |** *template-name* **v2}** command in interface configuration mode to enable Second-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Second-Generation Web Authentication relies on AAA. Enable AAA before you implement the former.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host is responsible for authenticating users.

Configuring an AAA Method List for Second-Generation Web Authentication

By default, no AAA method list is configured for Second-Generation Web Authentication.

Run the **aaa authentication web-auth** command in global configuration mode to configure an AAA method list for Second-Generation Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

Configuring an AAA Method List for Second-Generation Web Accounting

By default, no AAA method list is configured for Second-Generation Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Second-Generation Web Accounting.

The AAA method list for Web accounting is used for accounting interaction during the Webauth process.

Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

Specifying the UDP Port of the Portal Server

By default, UDP Port 50100 is used.

Run the **port** command in template configuration mode to specify the UDP port of the portal server.

The UDP port is specified for the portal server to communicate with the NAS.

5.4 Configuration

Configuration	Description and Command

Configuration	Description and Command	
Configuring First-Generation Web Authentication	(Mandatory) It is used to set the basic parameters of First-Generation Web Authentication.	
	web-auth template eportalv1	Configures the first-generation Webauth template.
	ip {*ip-address*}	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	snmp-server community { *community-string* } **rw**	Configures the SNMP-server community string.
	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	Configures the SNMP-server host.
	snmp-server enable traps web-auth	Enables the SNMP-server Trap/Inform function.
	web-auth enable	Enables First-Generation Web Authentication on an interface.
Configuring Second-Generation Web Authentication	(Mandatory) It is used to set the basic parameters of Second-Generation Web Authentication.	
	aaa new-model	Enables AAA.
	radius-server host {*ip-address*}[**auth-port** *port-number*] [**acct-port** *port-number*] **key** {*string*}	Configures the RADIUS-server host and communication key.
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Web authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Web Accounting. (RADIUS accounting is implemented.)
	web-auth template{**eportalv2** |*portal-name***v2**}	Configures a second-generation Webauth template.
	ip {*ip-address*}	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.

Configuration	Description and Command	
	web-auth enable{ **eportalv2 |** *template-name* }	Enables Second-Generation Web Authentication on an interface.
Specifying an Authentication Method List	(Optional) It is used to specify an AAA authentication method list in template configuration mode. The name of the method list must be correctly specified.	
	authentication { *mlist-name* }	Specifies an AAA authentication method list(only for Second-Generation Web Authentication and iPortal Web Authentication.)
Specifying an Accounting Method List	(Optional) It is used to specify an AAA accounting method in template configuration mode. The name of the method list must be correctly specified.	
	accounting { *mlist-name* }	Specifies an AAA accounting method list(only for Second-Generation Web Authentication and iPortal Web Authentication.)
Configuring the Communication Port of the Portal Server	(Optional) It is used to specify the UDP port of the portal server in template configuration mode. The configured port number must be consistent with that on the RADIUS server.	
	port { *port-num* }	Configures the communication port of the portal server.
Specifying the Webauth Binding Mode	(Optional) It is used to specify the entry binding mode in template configuration mode.	
	bindmode {ip-mac-mode | ip-only-mode}	Specifies the template binding mode.
Configuring the Format of the Webauth URL	(Optional) It is used to configure the redirection URL format for a template.	
	fmt custom encry { [**none | md5 | des | des_ecb | des_ecb3**] } { [**user-ip** *userip-str*] [**user-mac** *usermac-str* **mac-format [dot | line | none]**] [**user-vid** *uservid-str*] [**user-id userid-str**] [**nas-ip** *nasip-str*] [**nas-id** *nasid-str* **][nas-id2***nasid2-str* **][ac-name** *acname-str*] [**ap-mac** *apmac-str* **mac-format [dot | line | none]**] [**url** *url-str*] [**ssid** *ssid-str*] [**port** *port-str*] [**ac-serialno** *ac-sno-str*] [**ap-serialno** *ap-sno-str*] [**additional** *extern-str*] }	Configures the format of the Webauth URL.
Configuring the Redirection HTTP Port	(Optional) It is used to configure the TCP interception port for redirection, so that the packets on the specified port can be redirected when interception is enabled.	
	http redirect port { *port-num* }	Configures the redirection TCP port.

Configuration	Description and Command	
Configuring Rate Limit Webauth Logging	(Optional) It is used to configure the syslog function in Web authentication.	
	web-auth logging enable {*num* }	Configures the rate limit Webauth logging.
Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients	(Optional) It is used to adjust the HTTP session limit. The limit value needs to be increased when there are many sessions in the background.	
	http redirect session-limit { *session-num* } [**port** { *port-session-num* }]	Configures the maximum number of HTTP sessions for unauthenticated clients.
Configuring the HTTP Redirection Timeout	(Optional) It is used to modify the timeout period for redirection connections. The timeout needs to be increased to complete redirection when the network condition is bad.	
	http redirect timeout{ *seconds* }	Configures the HTTP redirection timeout.
Configuring the Straight-Through ARP Resource Range	(Optional) It is used to permit the ARP of the specified addresses to pass. The gateway ARP must be permitted to pass when ARP check is enabled.	
	http redirect direct-arp { *ip-address* [*ip-mask*]}	Configures the straight-through ARP resource.
Configuring an Authentication-Exempted Address Range	(Optional) It is used to exempt clients from authentication when accessing the Internet.	
	web-auth direct-host { *ip-address* [*ip-mask*] [**arp**] }	Configures the range of the IP or MAC addresses of clients free from authentication.
Configuring the Interval for Updating Online User Information	(Optional) It is used to configure the interval for updating online user information.	
	web-auth update-interval *{ seconds }*	Configures the interval for updating online user information.
Configuring Portal Detection	(Optional) It is used to detect the availability of the portal server. If it is not available, the services are switched to the standby portal server. This function must be used together with portal standby function.	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries**]**	Configures the portal server detection interval, timeout period, and timeout retransmission times.
Configuring Portal Escape	(Optional) It is used to allow new clients to access the Internet without authentication when the portal server is not available.	
	web-auth portal-escape	Configures portal escape.
Enabling DHCP Address Check	(Optional) It is used to check whether the IP address of a client is allocated by the DHCP server. If not, the client's authentication request is denied.	

Configuration	Description and Command	
	web-auth dhcp-check	Checks whether the IP address of a client is assigned by the DHCP server.
Configuring the Portal Communication Port	⚠ (Optional) It is used to configure the port (source port) used for the communication between the NAS and portal server.	
	ip portal source-interface *interface-type interface-num*	Specifies the port used for the communication between the NAS and portal server.
Configuring VLAN-Based Authentication on a Port	⚠ (Optional) It is used to configure the VLAN in which only the STAs inside the configured VLAN cannot initiate Web authentication.	
	web-auth vlan-control *vlan-list*	Configures the VLAN-based authentication on a port.

5.4.1 Configuring First-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

↘ Configuring the Portal Server

- (Mandatory)To enable Web authentication successfully, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

↘ Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

↘ Setting the SNMP Parameters Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must set the SNMP network management parameters used for the communication between the NAS and portal server.
- The NAS or convergence device and portal server jointly manage authenticated clients through SNMP/MIB. A table of authenticated clients is managed by MIB on the NAS. The portal server is able to access the MIB to obtain client statistics so as to control client login and logout. When a client logs out, the NAS or convergence device will inform the portal server by Webauth Inform packets.

Enabling First-Generation Web Authentication on an Interface

- Mandatory.
- When First-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring the First-Generation Webauth Template

Command	**web-auth template eportalv1**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**eportalv1** is the default template of First-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** {*ip-address*}
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** {*url-string*}
Parameter Description	*url-string*: Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode

Usage Guide	The URL starts with **http://** or **https://**.

Specifying the Webauth Binding Mode

Command	**bindmode** { **ip-mac-mode | ip-only-mode** }
Parameter Description	Indicates the Webauth binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth Communication Key

Command	**web-auth portal key** {*key-string*}
Parameter Description	*key-string:* Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the SNMP-Server Community String

Command	**snmp-server community** {*community-string*}**rw**
Parameter Description	*community-string*: Indicates the community string. **rw**: Must be set to **rw** to support the read and write operations as the Set operation on MIB is required.
Command Mode	Global configuration mode
Usage Guide	The SNMP-server community string is used by the portal server to manage the online clients on the NAS or convergence device.

Configuring the SNMP-Server Host

Command	**snmp-server host** {*ip-address*} **inform version 2c** {*community-string*} **web-auth**
Parameter Description	*ip-address*: Indicates the IP address of the SNMP-server host, that is, the portal server. *community-string*: Configures the community string used to send an SNMP Inform message.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP-server host to receive Webauth messages, including the type, version, community string, and other parameters. **inform:** Enables the SNMP Inform function. The NAS or convergence device will send a message to the portal server when a client logs out. The message type is set to Inform instead of Trap to avoid message loss. **version 2c**: Indicates SNMPv2 for SNMP Inform is not supported in all SNMP versions excluding SNMPv1. **web-auth**: Indicates the preceding parameters to be used for Web authentication.

	For details regarding SNMP configuration and others, see the *Configuring SNMP*. The SNMP parameter **version 2c**listed here is aimed at SNMPv2. SNMPv3 is recommended if higher security is required for the SNMP communication between the NAS and portal server. To use SNMPv3, change **SNMP Community** to **SNMP User**, **version 2c** to **SNMPv3**, and set SNMPv3-related security parameters. For details, see the *Configuring SNMP*.

Enabling the Webauth Trap/Inform Function

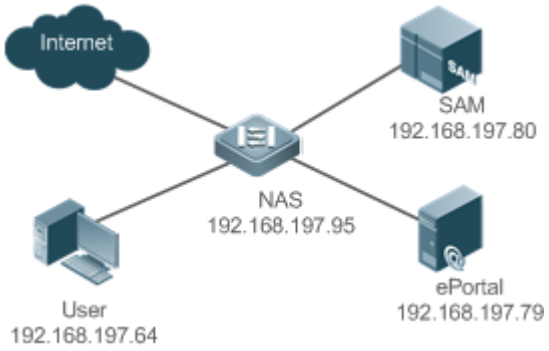
Command	**snmp-server enable traps web-auth**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the NAS or convergence device to send Webauth Trap and Inform messages externally. web-auth: Indicates Web authentication messages.

Enabling First-Generation Web Authentication on an Interface

Command	**web-auth enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring First-Generation Web Authentication

Scenario **Figure 5-4**	
Configuration Steps	● On the NAS, configure the IP address of the ePortal server and the key (test) used for communicating with the ePortal server. ● Configure the Webauth URL on the NAS.

	● Set the SNMP network management parameters (community string: public) used for the communication between the NAS and ePortal server. ● Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	Hostname# config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#web-auth template eportalv1 Hostname(config.tmplt.eportalv1)#ip 192.168.197.79 Hostname(config.tmplt.eportalv1)#exit Hostname(config)# web-auth portal key test
	Hostname(config)# web-auth template eportalv1 Hostname(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp Hostname(config.tmplt.eportalv1)#exit
	Hostname(config)# snmp-server community public rw Hostname(config)# snmp-server enable traps web-auth Hostname(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth Hostname(config)# exit
	Hostname(config)# interface range GigabitEthernet 0/2-3 Hostname(config-if-range)# web-auth enable Hostname(config-if-range)# exit
Verification	● Check whether Web authentication is configured successfully.
	Hostname(config)#show running-config … snmp-server host 192.168.197.79 inform version 2c public web-auth snmp-server enable traps web-auth snmp-server community public rw … web-auth template eportalv1 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp !

	web-auth portal key test … interface GigabitEthernet 0/2 web-auth enable ! interface GigabitEthernet 0/3 web-auth enable
	Hostname#show web-auth control Port Control Server Name Online User Count ------------------------- -------- ---------------------- ------------------ … GigabitEthernet 0/20n eportalv1 0 GigabitEthernet 0/30n eportalv1 0 …
	Hostname#show web-auth template Webauth Template Settings: --- Name: eportalv1 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v1 ……

Common Errors

- The SNMP parameters used for the communication between the portal server and NAS are configured incorrectly, causing authentication failures.
- Specify the IP-MAC binding mode to deploy Web authentication on layer-3 networks, causing authentication failures.
- When Web authentication is used in conjunction with VRRP, run the snmp-server trap-source ip command to specify the VRRP address; otherwise, the portal server cannot process Trap packets correctly.

5.4.2 Configuring Second-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. IPv6 is supported.

Notes

- Second-Generation Web Authentication complies with the CMCC WLAN Service Portal Specification. Furthermore, it is extended to support our company's portal server. Perform compatible configuration based on the server performance in actual deployment. For details, see the subsequent chapter.
- The cmcc-normal and cmcc-ext1 parameters in the fmt command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid.

Configuration Steps

Enabling AAA

- (Mandatory) To enable Second-Generation Web Authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Second-Generation Web Authentication.

Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable Second-Generation Web Authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Configuring an AAA Method List for Web Authentication

- (Mandatory) To enable Second-Generation Web Authentication, you must configure an AAA authentication method list.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

Configuring an AAA Method List for Web Accounting

- (Mandatory) To enable Second-Generation Web Authentication, you must configure an AAA method list for Web accounting.
- An accounting method list is used to associate an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the Portal Server

- (Mandatory) To enable Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the

portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Configuring the Portal Server in Global or Interface Configuration Mode

- (Mandatory) To enable Second-Generation Web Authentication, you must specify the use of the second generation portal server in global or interface configuration mode.
- The NAS first selects the portal server in interface configuration mode. If such a portal server does not exist, the NAS selects the portal server in global configuration mode. If such a portal server does not exist, eportalv1 is used by default. The NAS redirects users to the selected portal server.

Enabling Second-Generation Web Authentication on an Interface

- Mandatory.
- When Second-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** {*ip-address*} [**auth-port***port-number1*] [**acct-port** *port-number2*] **key** {*string*}
Parameter	*ip-address*: Indicates the IP address of the RADIUS server host.

Description	*port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	Second-Generation Web Authentication adopts the RADIUS authentication method.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	Second-Generation Web Authentication adopts the RADIUS accounting method.

Configuring the Second-Generation Webauth Template

Command	**web-auth template**{**eportalv2 |** *portal-name* **v2**}
Parameter Description	*portal-name*: Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of Second-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** { *url-string* }
Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt** {**cmcc-ext1	cmcc-ext2	cmcc-mtx	cmcc-normal	ct-jc	cucc| Hostname	custom**}
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	The **cmcc-normal** and **cmcc-ext1** parameters in the **fmt** command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid. The **cmcc-ext2** is supported for Liaoning CMCC. When **fmt** is set to **cmcc-mtx**, the URL format of mobile AC vendors is supported. The **ct-jc** format is supported for Chine Telecom. The **cucc** format is supported for Shandong China Telecom. The **custom** format is defined by users.

Specifying the Webauth Binding Mode

Command	**bindmode** { **ip-mac-mode	ip-only-mode** }
Parameter Description	Indicates the Webauth binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth Communication Key

Command	**web-auth portal key** { *key-string* }
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

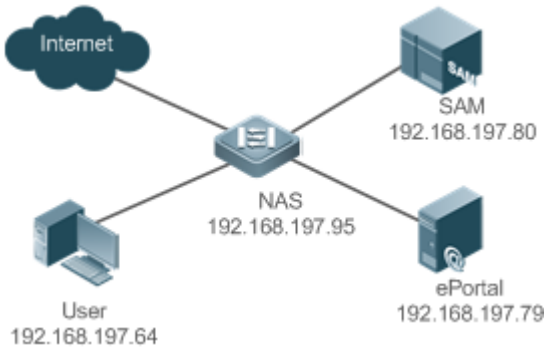
Enabling Second-Generation Web Authentication on an Interface

Command	**web-auth enable** {**eportalv2 |** *template-name*}

Parameter Description	Indicates a Webauth template.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Second-Generation Web Authentication

Scenario Figure 5-5	
Configuration Steps	• Enable AAA on the NAS. • Configure the RADIUS-server host and communication key on the NAS. • Configure the default AAA method lists for Web authentication and accounting on the NAS. • Configure the IP address of the portal server and the Webauth communication key used for communicating with the portal server on the NAS. • Configure the Webauth URL on the NAS. • Configure Second-Generation Web Authentication in global configuration mode on the NAS. • Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#aaa new-model
	Hostname(config)#radius-server host 192.168.197.79 key test
	Hostname(config)#aaa authentication web-auth default group radius Hostname(config)#aaa accounting network default start-stop group radius
	Hostname(config)#web-auth template eportalv2 Hostname(config.tmplt.eportalv2)#ip 192.168.197.79 Hostname(config.tmplt.eportalv2)#exit Hostname(config)#web-auth portal key test

	Hostname(config)# web-auth template eportalv2 Hostname(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp Hostname(config.tmplt.eportalv2)#exit
	Hostname(config)# interface range GigabitEthernet 0/2-3 Hostname(config-if-range)# web-auth enable eportalv2 Hostname(config-if-range)# exit
Verification	● Check whether Web authentication is configured successfully.
	Hostname(config)#show running-config … aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius … radius-server host 192.168.197.79 key test … web-auth template eportalv2 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp ! web-auth portal key test … interface GigabitEthernet 0/2 web-auth enable eportalv2 ! interface GigabitEthernet 0/3 web-auth enable eportalv2
	Hostname#show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- …

	GigabitEthernet 0/2 On eportalv2 0 GigabitEthernet 0/3 On eportalv2 0 ...
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 50100 State: Active Acctmlist: default Authmlist: default ...

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the *CMCC WLAN Service Portal Specification*, causing compatibility failure.

5.4.3 Specifying an Authentication Method List

Configuration Effect

- The portal server sends an authentication request to the NAS when a user submits authentication information. The NAS resolves the authentication server information and other information based on the configured authentication method list name before initiating authentication.
- The NAS selects the authentication server based on the specified authentication method list.

Notes

- Before you configure an authentication method list name, ensure that the authentication methods in the list have been configured on the AAA module. The command used to configure authentication methods on the AAA module is **aaa authentication web-auth** { *default* | *list-name* }*method1* [*method2*...].

Configuration Steps

- Optional.
- The default authentication method is used if no authentication method list is configured. Run the **authentication** { *mlist-name* } command to configure an authentication method list name when the authentication method list name on the AAA module needs to be modified or multiple method lists exist.

Verification

- Configure two authentication method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Create user a and configured a password for the user on server 1. Create user b on server 2.
- Configure the use of list 1.
- Perform authentication as user b and check that authentication fails.
- Perform authentication as user a and check that authentication is successful.

Related Commands

Specifying an Authentication Method List

Command	**authentication** {*mlist-name*}
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured authentication method list name is consistent with that on the AAA module.

Configuration Example

Specifying an Authentication Method List

Configuration Steps	● Specify the authentication method list **mlist1**.
	`Hostname(config.tmplt.iportal)#authentication mlist1`
Verification	● Check whether the configuration is successful.

	`Hostname#show web-auth template`
	`Webauth Template Settings:`
	`----------`
	`Name: eportalv2`
	`Url: http://17.17.1.21:8080/eportal/index.jsp`
	`Ip: 17.17.1.21`

Configuration Steps	● Specify the authentication method list **mlist1**.
	`Hostname(config.tmplt.iportal)#authentication mlist1`
Verification	● Check whether the configuration is successful.

	`BindMode: ip-only-mode`
	`Type: v2`
	`Port: 50100`
	`State: Active`
	`Acctmlist: default`
	`Authmlist: mlist1`

5.4.4 Specifying an Accounting Method List

Configuration Effect

- The NAS sends an accounting request when a user passes authentication. The recipient of the request depends on the configuration of the accounting method list and is usually the portal server.
- Specify an accounting method list for the NAS to perform accounting.

Notes

- Ensure that the accounting method list has been configured on the AAA module. The command used to configure accounting methods on the AAA module is **aaa accounting network** {**default** | *list-name* }start-stop method1 [method2...].

Configuration Steps

- Optional.
- The default accounting method is used if no accounting method list is configured. Run the **accounting** {*mlist-name* } command to configure an accounting method list name when the accounting method list name on the AAA module needs to be modified or multiple method list names exist.

Verification

- Configure two accounting method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Configure the use of list 1.
- Use a valid account to perform authentication to access the Internet.
- View user accounting information on server1 and server2. Check that the user accounting information exists only on server1.

Related Commands

Specifying an Accounting Method List

Command	**accounting**{*mlist-name*}
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured accounting method list name is consistent with that on the AAA module.

Configuration Example

Specifying an Accounting Method List

Configuration Steps	● Specify the accounting method list **mlist1**.
	`Hostname(config.tmplt.eportalv2)#accounting mlist1`
Verification	● Check whether the configuration is successful.

	`Hostname#show web-auth template`
	`Webauth Template Settings:`
	`----------`
	`Name: eportalv2`
	`Url: http://17.17.1.21:8080/eportal/index.jsp`
	`Ip: 17.17.1.21`
	`BindMode: ip-mac-mode`
	`Type: v2`
	`Port: 50100`
	`State: Active`
	`Acctmlist: mlist1`
	`Authmlist: mlist1`

5.4.5 Configuring the Communication Port of the Portal Server

Configuration Effect

- When the NAS detects that a user logs out, it notifies the portal server. The NAS interacts with the portal server through the portal specification, which specifies the port number used to listen to and send/receive packets.

- When the listening port of the portal server is changed, the communication port of the portal server must be modified on the NAS to enable the NAS to interact with the portal server.

Notes

- The configured port number must be consistent with the port actually used by the portal server.
- This function is applicable to Hostname Second-Generation Web Authentication. The two authentication schemes use different default port numbers. In Hostname Second-Generation Web Authentication, the configured port number is used for the interaction between the NAS and portal server through the portal specification.

Configuration Steps

- Optional.
- Run the **port** *port-num* command to maintain port configuration consistency when the portal server does not use the default port number or the listening port of the NAS conflicts with other port and needs to be adjusted.

Verification

- Configure Hostname Second-Generation Web Authentication.
- Change the listening port of the server to 10000.
- Run the **port** *port-num* command to configure the port number 10000.
- Simulate the scenario where a user performs authentication to access the Internet.
- Force the user offline on the NAS, refresh the online page, and check that a user logout notification is displayed.

Related Commands

Configuring the Communication Port of the Portal Server

Command	**port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Communication Port of the Portal Server

Configuration Steps	● Configure the communication port of the portal server as port 10000.
	`Hostname(config.tmplt.eportalv2)#port 10000`
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure the communication port of the portal server as port 10000.
	`Hostname(config.tmplt.eportalv2)#port 10000`
Verification	● Check whether the configuration is successful.

	`Hostname#show web-auth template`
	`Webauth Template Settings:`
	`----------`
	`Name: eportalv2`
	`Url: http://17.17.1.21:8080/eportal/index.jsp`
	`Ip: 17.17.1.21`
	`BindMode: ip-only-mode`
	`Type: v2`
	`Port: 10000`
	`Acctmlist:`
	`Authmlist:`

5.4.6 Specifying the Webauth Binding Mode

Configuration Effect

- When a user goes online, the user's entry needs to be written to a forwarding rule. The forwarding rule mapping method can be modified by specifying different binding modes, which further affects the Internet access rules applied to users. In IP-only mode, all the packets carrying the specified IP address are permitted to pass, and the STAs who send the packets can access the Internet. In IP+MAC mode, only the packets carrying both the specified IP address and MAC address are permitted to pass, and the STAs who send the packets can access the Internet.

Notes

- In Layer-3 authentication, the MAC addresses visible to the NAS are the gateway addresses of STAs. Because these MAC addresses are not accurate, the IP-only mode should be used.

Configuration Steps

- (Optional) The default Webauth binding mode is IP+MAC.
- Determine a binding mode based on the accuracy of user information obtained by the NAS. When the IP and MAC addresses of STAs are accurate (in L2 authentication, for example), IP+MAC is recommended. When the IP and MAC addresses are not accurate, select IP-only.

Verification

- Change the binding mode to IP-only.
- Simulate the scenario where a user performs authentication to access the Internet.
- Modify the MAC address of the user, or use a client with the same IP address but a different MAC address to access the Internet.
- Check that the user accesses the Internet normally.

Related Commands

Specifying the Webauth Binding Mode

Command	**bindmode {ip-mac-mode | ip-only-mode}**
Parameter Description	**ip-mac-mode**: Indicates IP-MAC binding mode. **ip-only-mode**: Indicates IP-only binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Specifying the Webauth Binding Mode

Configuration Steps	● Set the binding mode to IP-only.
	`Hostname(config.tmplt.eportalv2)#bindmode ip-only-mode`
Verification	● Check whether the configuration is successful.

	`Hostname#show web-auth template`
	`Webauth Template Settings:`
	`----------`
	`Name: eportalv2`
	`Url: http://17.17.1.21:8080/eportal/index.jsp`
	`Ip: 17.17.1.21`
	`BindMode: ip-only-mode`
	`Type: v2`
	`Port: 10000`
	`Acctmlist:`
	`Authmlist:`

5.4.7 Configuring the Redirection HTTP Port

Configuration Effect

- When an STA accesses network resources (for example, the user accesses the Internet using a browser), the STA sends HTTP packets. The NAS or convergence device intercepts these HTTP packets to determine whether the STA is accessing network resources. If the NAS or convergence device detects that the STA is not authenticated, it prevents the STA from accessing network resources and displays an authentication page to the STA. By default, the NAS intercepts the HTTP packets that STAs send to port 80 to determine whether STAs are accessing network resources.
- After a redirection HTTP port is configured, the HTTP requests that STAs send to the specified destination port can be redirected.

Notes

- The commonly used management ports on the NAS 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. All ports except port 80 with numbers smaller than 1000 are seldom used by the HTTP protocol. To avoid a conflict with the well-known TCP port, do not configure a port with a small number as the redirection port unless necessary.

Configuration Steps

- Optional.
- When you configure automatic client acquisition, if you need to enable the NAS to intercept the HTTP packets that STAs send to the specified destination port, configure a redirection HTTP port.

Verification

- Configure an interception port.
- Open the browser of a PC and access the Internet through the port without performing authentication.
- Check whether the access requests are redirected to an authentication page.

Related Commands

↘ Configuring the Redirection HTTP Port

Command	**http redirect port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Global configuration mode
Usage Guide	A maximum of 10 different destination port numbers can be configured, not including default ports 80 and 443.

Configuration Example

↘ Configuring the Redirection HTTP Port

Configuration Steps	● Configure port 8080 as the redirection HTTP port.
	`Hostname(config)#http redirect port 8080`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth rdport`
	`Rd-Port:`
	`80 443 8080`

5.4.8 Configuring Rate Limit Webauth Logging

Configuration Effect

- The Web authentication module sends syslog messages to the administrator to display the information and relevant events of users who perform login/logout. By default, syslog messages are shielded.
- After syslog output rate limiting is configured, syslog messages are sent at a certain rate.

Notes

- When the login/logout rate is high, syslog messages are output frequently, which affects device performance and results in spamming.

Configuration Steps

- Optional.
- Configure syslog output rate limiting when you need to view the syslog messages about user login/logout.

Verification

- Configure logging rate limiting.
- Check whether users log in and out at a certain rate.
- Check that syslog messages are printed out at the limit rate.

Related Commands

↘ **Configuring Rate Limit Webauth Logging**

Command	**web-auth logging enable** *num*
Parameter Description	*num*: Indicates the syslog output rate (entry/second).
Command Mode	Global configuration mode
Usage Guide	When the syslog output rate is set to **0**, syslog messages are output without limit. The output of syslog

	messages of the critical level and syslog messages indicating errors is not limited.

Configuration Example

↘ Configuring Rate Limit Webauth Logging

Configuration Steps	● Disable rate limit Webauth Logging.
	`Hostname(config)#web-auth logging enable 0`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth logging enable 0`
	`...`

5.4.9 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Effect

- When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The NAS 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, it is necessary to limit the maximum number of HTTP sessions that the unauthenticated user can initiate on the NAS.
- A user occupies an HTTP session when performing authentication, and the other application programs of the user may also occupy HTTP sessions. For this reason, it is recommended that the maximum number of HTTP sessions for an unauthenticated user be not set to 1. By default, each unauthenticated user can initiate 255 HTTP sessions globally, and each port supports up to 300 HTTP sessions initiated by unauthenticated clients.

Notes

- 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 may occupy HTTP sessions and then perform Web authentication again.

Configuration Steps

- Optional.
- Perform this configuration when you need to change the maximum number of HTTP sessions that each unauthenticated user can initiate and the maximum number of HTTP sessions that unauthenticated clients can initiate on each port.

- Perform this configuration when you configure automatic SU client acquisition.

Verification

- Modify the maximum number of HTTP sessions that an unauthenticated user can initiate.
- Simulate the scenario where an unauthenticated user constructs identical sessions to connect to the NAS continuously.
- Simulate the scenario where the unauthenticated user accesses the Internet using a browser. Check whether the access requests are redirected and the NAS notifies the user that the maximum number of sessions is reached.

Related Commands

Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Command	**http redirect session-limit** { *session-num* }[**port** { *port-session-num* }]
Parameter Description	*session-num*: Indicates the maximum number of HTTP sessions for unauthenticated clients. The value range is 1 to 255. The default value is 255. *port-session-num*: Indicates the maximum number of HTTP sessions on each port for authenticated clients. The value range is 1 to 65,535. The default value is 300.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Steps	● Set the maximum number of HTTP sessions for unauthenticated clients to 3.
	`Hostname(config)#http redirect session-limit 3`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth parameter`
	`HTTP redirection setting:`
	`  session-limit: 3`
	`  timeout:  3`
	`Hostname(config)#`

5.4.10 Configuring the HTTP Redirection Timeout

Configuration Effect

- Configure the HTTP redirection timeout to maintain redirection connections. When an unauthenticated user tries to access network resources through HTTP, the TCP connection requests sent by the user will be intercepted and

re-established with the NAS or convergence device. Then, the NAS or convergence device waits for the HTTP GET/HEAD packets from the user and responds with HTTP redirection packets to close the connection. The redirection timeout is intended to prevent the user from occupying the TCP connection for a long time without sending GET/HEAD packets. By default, the timeout for maintaining a redirection connection is 3s.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to change the timeout for maintaining redirection connections.

Verification

- Change the timeout period.
- Use a network packet delivery tool to set up a TCP connection.
- View the status of the TCP connection on the NAS. Check whether the TCP connection is closed when the timeout is reached.

Related Commands

Configuring the HTTP Redirection Timeout

Command	**http redirect timeout** { *seconds* }
Parameter Description	*Seconds*: Indicates the timeout for maintaining redirection connections, in the unit of seconds. The value ranges from 1 to 10. The default value is 3s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the HTTP Redirection Timeout

Configuration Steps	● Set the HTTP redirection timeout to 5s.
	`Hostname(config)#http redirect timeout 5`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth parameter`
	`HTTP redirection setting:`
	`  session-limit: 255`

Configuration Steps	● Set the HTTP redirection timeout to 5s.
	`Hostname(config)#http redirect timeout 5`
Verification	● Check whether the configuration is successful.
	`timeout: 5`

5.4.11 Configuring the Straight-Through Network Resources

Configuration Effect

- After Web authentication or 802.1Xauthentication is enabled on a port, the users connecting to the port need to pass Web authentication or 802.1Xauthentication before accessing network resources.
- Perform this configuration to exempt users from authentication when accessing some network resources.
- If a website is configured as a network resource of authentication exemption, all users, including unauthenticated clients, can access the website. By default, authentication exemption is not configured, and unauthenticated clients are not allowed to access network resources.

Notes

- The maximum number of free resources and the maximum number of unauthenticated clients cannot exceed 1000 respectively. 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 set.
- **http redirect direct-site** is used to configure the straight-through URL address for users, and **http redirect** is used to configure the straight-through IP address of the Web authentication server. The addresses configured using the two commands can be accessed without authentication, but they have different usages. It is recommended not to configure the IP address of the Web authentication server by using **http redirect direct-site**.

Configuration Steps

- Optional.
- Run the **http redirect direct-site** command to enable unauthenticated clients to access network resources.

Verification

- Configure the straight-through network resources.
- Check whether unauthenticated clients can access the configured network resources using PCs.

Related Commands

↘ Configuring the Straight-Through Network Resources

Command	**http redirect direct-site** { *ipv4-address* [*ip-mask*] [**arp**] }
Parameter	*ipv4-address*: Indicates the IPv4 address of the network exempt from authentication.

Description	*ip-mask*: Indicates the mask of the IPv4 address of the network exempt from authentication.
Command Mode	Global configuration mode
Usage Guide	To set authentication-exempted ARP resource, use the **http redirect direct-arp** command preferentially.

Configuration Example

↘ Configuring the Straight-Through Network Resources

Configuration Steps	● Configure the straight-through network resources as 192.168.0.0/16.
	`Hostname(config)#http redirect direct-site 192.168.0.0 255.255.0.0`
	● Set the range of consecutive networks exempt from authentication to 10.0.0.1-12.0.0.1. Hostname(config)# http redirect direct-site range 10.0.0.1 12.0.0.1
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth direct-site`
	`Direct sites:`
	`Address Mask ARP Binding Group Description`
	`--- --- --- --- ---`
	`192.168.0.0 255.255.0.0 Off N/A N/A`
	`Hostname(config)#`

5.4.12 Configuring the Straight-Through ARP Resource Range

Configuration Effect

When ARP check or similar functions are enabled, the ARP learning performed by clients is controlled. As a result, clients cannot learn the ARPs of the gateway and other devices, which affects user experience. You can configure the straight-through ARP resource range to permit the ARP learning packets destined for the specified address to pass.

Notes

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the Layer-2 access device as a straight-through ARP resource. Note the following point when you perform the configuration:
- When you configure straight-through websites and ARP resources in the same address or network segment, the **http redirect direct-arp** command automatically combines the websites and ARP resources. If no ARP option is specified for the configured websites, an ARP option will be automatically added after the combination.
- When ARP check is enabled, if the outbound addresses of the PCs connecting to the Layer-2 access device are not the gateway address, configure the outbound addresses as straight-through ARP resources. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.

Configuration Steps

- Optional.
- If ARP check is enabled on the NAS, you must configure the free resources and gateway address as straight-through ARP resources.

Verification

- Configure straight-through ARP resources.
- Clear the ARP cache of the PC of an unauthenticated user. (Run the **arp -d** command in the Windows operating system.)
- Run the **ping** command on the PC to access the straight-through ARP resources.
- View the ARP cache on the PC (run the **arp -a** command in the Windows operating system) and check whether the PC learns the ARP address of the straight-through ARP resources.

Related Commands

Configuring the Straight-Through ARP Resource Range

Command	**http redirect direct-arp** {*ip-address* [*ip-mask*]}
Parameter Description	*ip-address*: Indicates the IP address of free resources. *ip-mask*: Indicates the mask of free resources.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Straight-Through ARP Resource

Configuration Steps	● Configure the straight-through ARP resource as 192.168.0.0/16.
	`Hostname(config)#http redirect direct-arp 192.168.0.0 255.255.0.0`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth direct-arp`
	`Direct arps:`
	`  Address  Mask`
	`  --------------- ---------------`
	`  192.168.0.0  255.255.0.0`
	`Hostname(config)#`

5.4.13 Configuring an Authentication-Exempted Address Range

Configuration Effect

- Exempt users from Web authentication when accessing reachable network resources. By default, no authentication-exempted address range is configured. All users must pass Web authentication before accessing network resources.
- The authentication-exempted address range can be configured as an IP address range or MAC address range.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure an authentication-exempted user.
- Check whether the user can access the Internet without authentication.

Related Commands

Configuring an Authentication-Exempted Address Range

Command	**web-auth direct-host** { *ipv4-address* [*ipv4-mask*] [**arp**] [**port** *interface-name*]
Parameter Description	ipv4-address: Indicates the IPv4 address of the user exempt from authentication. ip-mask: Indicates the mask of the IPv4 address of the user exempt from authentication. *interface-name*: Indicates the name of the interface on which authentication exemption is enabled.
Command Mode	Global configuration mode
Usage Guide	The **arp** field is used to assign pass permissions to ARP packets. This field must be set when ARP check is enabled.

Configuration Example

Configuring an Authentication-Exempted Address Range

Configuration Steps	● Configure an authentication-exempted address range.
	`Hostname (config)# web-auth direct-host 192.168.197.64`
Verification	● Check whether the configuration is successful.

```
Hostname(config)#show web-auth direct-host
Direct hosts:
  Address         Mask            Port           ARP Binding   Group      Description
  --------------- --------------- -------------- ------------- ---------- ------------
  192.168.197.64  255.255.255.255                Off           N/A        N/A
Hostname(config)#
```

5.4.14 Configuring the Interval for Updating Online User Information

Configuration Effect

- The NAS or convergence device maintains and periodically updates the information of online users, including users' online duration, to monitor the usage of network resources. When the online duration threshold is reached, users will be prevented from using network resources.

Notes

- The user information updating interval must be configured as 60 or multiple of 60; otherwise, the system will select the minimum multiple of 60 above and closest to the actual configuration as the interval.

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure the interval for updating online user information.
- View the information of online users after the update interval has elapsed.

Related Commands

↘ Configuring the Interval for Updating Online User Information

Command	**web-auth update-interval** *{ seconds }*
Parameter Description	*seconds*: Indicates the interval for updating online user information, in the unit of seconds. The value ranges from 30 to 3,600. The default value is 180s.
Command Mode	Global configuration mode
Usage Guide	To restore the default updating interval, run the **no web-auth update-interval** command in global configuration mode.

Configuration Example

Configuring the Interval for Updating Online User Information

Configuration Steps	● Set the interval for updating online user information to 60s.
	`Hostname (config)# web-auth update-interval 60`
Verification	● Check whether the configuration is successful.
	`Hostname(config)#show run | include web-auth update-interval` `web-auth update-interval 60`

5.4.15 Configuring Portal Detection

Configuration Effect

- Detect the availability of the active portal server periodically. When the active portal server is unavailable, the standby portal server takes over the services.
- Hostname Second-Generation Web Authentication provides two detection methods. One is that 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. Another is the NAS sends ping packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Because some servers or intermediate network segments filter ping packets, the first method is commonly used. The ping detection method is only used based on special requirements. In Hostname First-Generation Web Authentication, the NAS connects to a port of the portal server and checks whether the port is reachable. If the portal is reachable, the NAS determines that the portal server is available.
- For the first method in the second-generation authentication, the interval of server availability detection is specified by the **interval** parameter, and the maximum number of packets that can be sent during each time of detection is specified by the **retransmit** parameter. If the portal server does not respond, the NAS determines that the portal server is unavailable. The timeout period for each packet is specified by the **timeout** parameter. The parameter settings are also supported by Hostname First-Generation Web Authentication.
- Portal server detection takes effect for Hostname First- and Second-Generation Web Authentication.
- If multiple portal servers are configured, these servers are working in active/standby mode.

Notes

- Multiple portal servers must be configured to realize failover when an error is detected on one server.
- Only one of the two detection methods can be used at a time in case of collision. If both detection methods are configured, a detection algorithm conflict will occur or the detection results will be inaccurate.
- The system will automatically select a detection method based on whether Hostname First- or Second-Generation Web Authentication is used.

Configuration Steps

- Optional.
- Configure multiple portal server templates applicable to Hostname First- or Second-Generation Web Authentication.

Verification

- Configure two portal server templates for Hostname First- or Second-Generation Web Authentication. Make the first template point to an unavailable server and the second template point to an available server.
- When the Console displays a log indicating that the portal server is not available, simulate the scenario where a user opens a browser to perform login authentication. Check whether the user is redirected to the second portal server.

Command	**web-auth portal-check** [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries**]**
Parameter Description	*intsec*: Indicates the detection interval. The default value is 10s. *tosec:* Indicates the packet timeout period. The default value is 5s. *intsec*: Indicates the timeout retransmission times. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	In many network environments, only one portal server is deployed, and portal server detection does not need to be configured. If multiple portal servers exist, it is recommended that the parameters of portal server detection be not set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.

Configuration Example

Configuring Portal Detection

Configuration Steps	● Configure portal detection.
	`Hostname(config)#web-auth portal-check interval 20 timeout 2 retransmit 2`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth portal-check interval 20 timeout 2 retransmit 2`
	`...`

5.4.16 Configuring Portal Escape

Configuration Effect

- Allow new users to access the Internet without authentication when the portal server is not available.

Notes

- To use the portal escape function, you must configure portal detection.
- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are not available.
- The escape function is intended only for the portal server, instead of the RADIUS server.

Configuration Steps

- Optional.
- Configure portal detection.
- Configure portal escape.
- (Optional) Configure the nokick attribute.

Verification

- Configure a portal server and disable the server.
- Configure the portal detection and escape functions.
- When the NAS detects that the portal server is not available, check whether a client accesses the Internet without authentication.

Related Commands

↘ Configuring Portal Escape

Command	**web-auth portal-escape [nokick]**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure portal escape if the continuity of some critical services on the network needs to be maintained when the portal server is faulty. You must configure portal detection when you use this function. If the nokick attribute is configured, the system does not force users offline when the escape function takes effect. If the nokick attribute is deleted, the system forces users offline.

Configuration Example

↘ Configuring Portal Escape

Configuration Steps	● Configure portal escape.
	`Hostname(config)#web-auth portal-escape`

Verification	• Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth portal-escape ...

5.4.17 Enabling DHCP Address Check

Configuration Effect

- Allow only the clients that are allocated with IP addresses through DHCP to perform authentication.

Notes

- To use the DHCP address check function, you must configure DHCP snooping.
- DHCP address check is supported only for IPv4.
- DHCP address check is applicable only to Hostname Second-Generation Web Authentication.
- The requirement that users obtain IP addresses through DHCP must be specified during network deployment. Those users cannot also use static IP addresses; otherwise, the existing users that use static IP addresses will be affected.
- If a few users need to use static IP addresses, configure these IP addresses as straight-through addresses, and these users are exempt from authentication.
- If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable the global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled in each interface.

Configuration Steps

- Optional.
- Enable DHCP snooping.
- Enable DHCP address check.

Verification

- Enable DHCP address check.
- Configure a static IP address that is not allocated by the DHCP server on a client.
- Connect the client to the Internet and check whether the STA cannot perform authentication.

Related Commands

↘ Enabling Global DHCP Address Check

Command	web-auth dhcp-check

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure DHCP address check to allow only the users who obtain IP addresses through DHCP to access the Internet. This function helps prevent the users who configure IP addresses without authorization from performing authentication to access the Internet.

Enabling Interface-based DHCP Address Check

Command	**web-auth dhcp-check {vlan [**vlan-list**]}**
Parameter Description	vlan-list: Indicates the VLAN range in which DHCP address check needs to be enabled in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable the global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled in each interface.

Configuration Example

Enabling DHCP Address Check

Configuration Steps	● Enable global DHCP address check.
	`Hostname(config)#web-auth dhcp-check`
Configuration Steps	● Enable interface-based DHCP address check.
	Hostname(config-if-TenGigabitEthernet 3/1)# web-auth dhcp-check vlan 1,3-4
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth dhcp-check`
	`...`
	`interface TenGigabitEthernet 3/1`
	`web-auth dhcp-check vlan 1,3-4`
	`...`

5.4.18 Configuring the Portal Communication Port

Configuration Effect

- Configure the port (source port) used for the communication between the NAS and portal server.

Notes

- Only one port can be configured for the communication between the NAS and portal server.

Configuration Steps

- Configure a port as the portal communication port.

Verification

- After Web authentication is enabled, capture a packet on the portal server during the authentication process and check whether the source IP address of the packet is the IP address of the specified port.

Related Commands

Configuring the Portal Communication Port

Command	**ip portal source-interface** *interface-type interface-num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Portal Communication Port

Configuration Steps	• Configure an aggregate port as the portal communication port.
	`Hostname(config)#ip portal source-interface Aggregateport 1`
Verification	• Check whether the configuration is successful.
	`Hostname(config)#show running-config` `ip portal source-interface Aggregateport 1`

5.4.19 Configuring VLAN-Based Authentication on a Port

Configuration Effect

- With this function enabled, clients in a VLAN configured on a port of the NAS can initiate authentication. Otherwise, the authentication will not start.

Notes

- This function supports configuration of multiple VLANs. If no VLAN is specified, Web authentication is implemented based on ports.

Configuration Steps

- Configure port-based Web authentication.
- Configure the VLAN for Web authentication.

Verification

- After Web authentication is enabled, specify the VLAN in which clients can initiate authentication. The HTTP packets sent outside the specified VLAN cannot be redirected.

Related Commands

↘ Configuring VLAN-Based Authentication on a Port

Command	**web-auth vlan-control** *vlan-list*
Parameter Description	*vlan-list*: Indicates the VLAN list to be authenticated.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring VLAN-Based Authentication on a Port

Configuration Steps	● Specify VLAN1 as the VLAN in which users can initiate authentication.
	`Hostname(config-if-GigabitEthernet 0/14)#web-auth vlan-control 1`
Verification	● Check whether the configuration is successful.
	`Hostname(config)#show running-config` `...`

Configuration Steps	● Specify VLAN1 as the VLAN in which users can initiate authentication.
	`Hostname(config-if-GigabitEthernet 0/14)#web-auth vlan-control 1`
Verification	● Check whether the configuration is successful.
	`web-auth vlan-control 1`

5.4.20 Upgrade Compatibility

Configuration Effect

- Some configuration commands are optimized in the 11.X series software and the command formats are changed. For details, see the subsequent description.
- The 10.X series software supports smooth upgrade without function loss. However, some commands are displayed in new formats after upgrade.
- When you run the commands in earlier formats in the **no** form in the 11.X series software, a message is displayed, indicating the **no** form is not supported. You need to perform the **no** operation in new command formats.

Configuration Steps

- It is recommended that you run commands in new formats.

Verification

- Check that function loss does not occur when the 10.X series software is upgraded to the 11.X series software, and commands are displayed and stored in new formats.
- The commands in new formats have the same functions as the commands in earlier formats.

Related Commands

↘ **Configuring the IP Address of the Portal Server in Hostname First-Generation Web Authentication**

Command	**http redirect** *ip-address*
Parameter Description	*url*: Indicates the ip address of the ePortal server in Hostname First-Generation Web Authentication.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 template, and the **ip** command in template configuration mode is executed to configure and display the IP address of the portal server. For details, see section 5.4.1"Configuring First-Generation Web Authentication."

↘ **Configuring the Portal Server**

Command	**portal-server [eportal1 | eportalv2]**

Parameter Description	**eportav1**: Indicates the information of the portal server used in Hostname First-Generation Web Authentication. **eportav2**: Indicates the information of the portal server used in Hostname Second-Generation Web Authentication.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 or eportalv2 template, and relevant information is filled in. The main parameters of the portal server include the IP address and URL of the server. The original command will be replaced by the **ip** command and **url** command in the template.

Configuring Web Authentication Control on a Port

Command	**web-auth port-control**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	In the 11.X version, the command is converted into **web-auth enable <type>**, in which **type** specifies the type (first or second generation) of Web authentication. The default type is Hostname First-Generation Web Authentication.

Configuring the IP-Only Binding Mode

Command	**web-auth port-control ip-only-mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 or eportalv2 template, depending on the actual configuration. The server binding mode is configured and displayed by using the **bindmode** command in template configuration mode. For details, see section 5.4.1 "Configuring First-Generation Web Authentication" and section 5.4.2 "Configuring Second-Generation Web Authentication."

Configuring VLAN-Based Web Authentication

Command	**web-auth allow-vlan** *list*
Parameter Description	*list*: Indicates the list of VLANs for which Web authentication is enabled.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into a command used to configure VLAN-based SCC authentication exemption.

Displaying the Configuration Information of Hostname First-Generation Web Authentication

Command	show http redirect
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	In the 11.X version, the command is unavailable and changed to **show web-auth template**.

Displaying the Port Control Information

Command	show web-auth port-control
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	In the 11.X version, the command is unavailable and changed to **show web-auth control**.

Configuration Example

Configuring Hostname First-Generation Web Authentication

Configuration Steps	● Check that the NAS runs on the 10.X version and is configured with the IP address of the portal server used by Hostname First-Generation Web Authentication.
	`Hostname(config)# http redirect 192.168.197.64`
	● Upgrade the NAS to 11.X.
Verification	● Run the **show running-config** command after the upgrade and check whether the new command formats are used.

	`Hostname#sh running-config`
	`web-auth template eportalv1`
	`  Ip 192.168.197.64`
	`!`

5.4.21 Configuring the Authenticated User Logout Delay on a Port

Configuration Effect

- Configure the delay after which the authenticated clients connected to a port go offline when the port fails.

Configuration Steps

Configuring the Authenticated User Logout Delay on a Port

- Configure the authenticated user logout delay on a port in global configuration mode.

Command	web-auth linkdown-timeout

Parameter Description	**timeout**: Indicates the logout delay. The default value is 60s.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check that the authenticated clients connected to the faulty port go offline after the configured time has elapsed.

Configuration Example

Configuring the Authenticated User Logout Delay on a Port

Configuration Steps	• Configure the logout delay. `Hostname(config)#web-auth linkdown-timeout {timeout}`
Verification	• Check whether the configuration is successful. `Hostname(config)#show running-config`

5.5 Monitoring

Clearing

Description	Command
Forces users offline.	**clear web-auth user** { **all | ip** *ip-address* | **mac** *mac-address* **| name** *name-string* **| session-id** *num* }
Clears all the straight-through network resources.	**clear web-auth direct-site**
Clears all the authentication-exempted users.	**clear web-auth direct-host**

Displaying

Description	Command
Displays the basic parameters of Web authentication.	**show web-auth parameter**
Displays the Webauth template configuration.	**show web-auth template**

Description	Command
Displays the authentication-exempted host range.	**show web-auth direct-host**
Displays the straight-through address range.	**show web-auth direct-site**
Displays the straight-through ARP range.	**show web-auth direct-arp**
Displays the TCP interception port.	**show web-auth rdport**
Displays the online information of all users or specified users.	**show web-auth user**{ **all | ip** *ip-address* | **mac** *mac-address* **| name** *name-string* }
Displays the Webauth mapping information.	**show web-auth ip-mapping**
Displays the Webauth portal check information.	**show web-auth portal-check**
Displays online and offline records about users.	show web-auth syslog ip *ip-address*

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs Web authentication.	**debug web-auth all**

6 Configuring SCC

6.1 Overview

The Security Control Center (SCC) provides common configuration methods and policy integration for various access control and network security services, so that these access control and network security services can coexist on one device to meet diversified access and security control requirements in various scenarios.

Typical access control services are dot1x, Web authentication, Address Resolution Protocol (ARP) check, and IP Source Guard. The network security services include Access Control List (ACL), Network Foundation Protection Policy (NFPP), and anti-ARP gateway spoofing. When two or more access control or network security services are simultaneously enabled on the device, or when both access control and network security services are simultaneously enabled on the device, the SCC coordinates the coexistence of these services according to relevant policies.

For details about the access control and network security services, see the related configuration guide. This document describes the SCC only.

Protocol and Standards

N/A

6.2 Application

Typical Application	Scenario
Access Control of Extended Layer 2 Campus Networks	Students on a campus network can access the Internet based on dot1x client authentication or Web authentication. ARP spoofing between the students should be prevented. In addition, terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

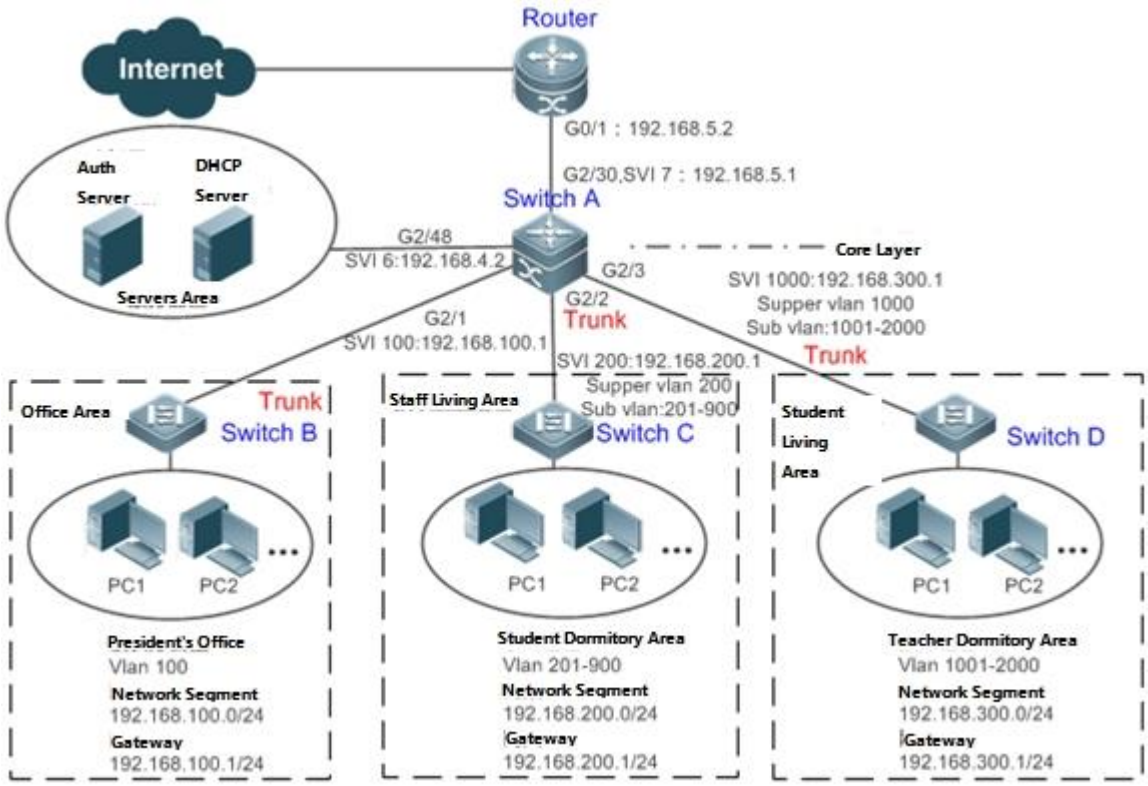
6.2.1 Access Control of Extended Layer 2 Campus Networks

Scenario

Students on a campus network of a university usually need to be authenticated through the dot1x client or Web before accessing the Internet, so as to facilitate accounting and guarantee the benefits of the university.

- The students can access the Internet through dot1x client authentication or Web authentication.
- ARP spoofing between the students is prevented, so as to guarantee the stability of the network.
- Terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

Figure 6-1



Remarks	A traditional campus network is hierarchically designed, which consists of an access layer, a convergence layer and a core layer, where the access layer performs user access control. On an extended Layer 2 campus network, however, user access control is performed by a core switch, below which access switches exist without involving any convergence device in between. The ports between the core switch and the access switches (such as switches B, C, and D in Figure 6-1) are all trunk ports. The user access switches B, C, and D connect to PCs in various departments via access ports, and VLANs correspond to sub VLANs configured on the downlink ports of the core switch, so that access users are in different VLANs to prevent ARP spoofing. The core switch A connects to various servers, such as the authentication server and the DHCP server. Super VLANs and sub VLANs are configured on the downlink ports. One super VLAN correspond to multiple sub VLANs, and each sub VLAN represents an access user.

Deployment

- On the core switch, different access users are identified by VLAN and port numbers. Each access user (or a group of access users) corresponds to one VLAN. The ports on each access switch that connect to downstream users are configured as access ports, and one user VLAN is assigned to each access user according to VLAN planning. The core switch does not forward ARP requests. The core switch replies to the ARP requests from authenticated users only, so as to prevent ARP spoofing. On the core switch A, user VLANs are regarded as sub VLANs, super VLANs are configured, and SVIs corresponding to the super VLANs are configured as user gateways.

- On the downlink ports of the core switch (switch A in this example) that connect to the teachers' living area and the students' living area, both dot1x authentication and Web authentication are enabled, so that users can freely select either authentication mode for Internet access.
- Any special department (such as the headmaster's office in this example) can be allocated to a particular VLAN, and this VLAN can be configured as an authentication-exemption VLAN so that users in this department can access the Internet without authentication.

6.3 Basic Concepts

Authentication-Exemption VLAN

Some special departments may be allocated to authentication-exemption VLANs to simplify network management, so that users in these departments can access network resources without authentication. For example, the headmaster's office can be divided into the authentication-exemption VLANs on the campus network, so that users in the headmaster's office can access the Internet without authentication.

IPv4 User Capacity

The number of IPv4 access users can be restricted to protect the access stability of online users on the Internet and improve the operational stability of the device.

The number of IPv4 access users is not restricted by default; that is, a large number of users can get online after being authenticated, till reaching the maximum hardware capacity of the device.

IPv4 access users include IP users (such as IP authenticated users) based on dot1x authentication, users based on Web authentication, and IP users manually bound (using IP source guard, ARP check, or other means).

Authenticated-User Migration

Online-user migration means that an online user can get authenticated again from different physical locations to access the network. On the campus network, however, for ease of management, students are usually requested to get authenticated from a specified location before accessing the Internet, but cannot get authenticated on other access ports. This means that the users cannot migrate. In another case, some users have the mobile office requirement and can get authenticated from different access locations. Then the users can migrate.

User Online-Status Detection

For a chargeable user, accounting starts immediately after the user passes the authentication and gets online. The accounting process does not end until the user actively gets offline. Some users, however, forget to get offline when leaving their PCs, or cannot get offline because of terminal problems. Then the users suffer certain economical losses as the accounting process continues. To more precisely determine whether a user is really online, we can preset a traffic value, so

that the user is considered as not accessing the Internet and therefore directly brought offline when the user's traffic is lower than the preset value in a period of time or there is not traffic of the user at all in a period of time.

Features

Feature	Function
Authentication-Exemption VLAN	Users in a specified VLAN can be configured as authentication-exemption users.
IPv4 User Capacity	The IPv4 user capacity of a specified interface can be restricted to guarantee the access stability of users on the Internet.
Authenticated-User Migration	You can specify whether the authenticated can migrate.
User Online-Status Detection	You can specify whether to detect the traffic of online users, so that a user is forced offline when the traffic of the user is lower than a preset value in a period of time.

6.3.1 Authentication-Exemption VLAN

Authentication-exemption VLANs are used to accommodate departments with special access requirements, so that users in these departments can access the Internet without authentication such as dot1x or Web authentication.

Working Principle

Suppose the authentication-exemption VLAN feature is enabled on a device. When the device detects that a packet comes from an authentication-exemption VLAN, access control is not performed. In this way, users in the authentication-exemption VLAN can access the Internet without authentication. The authentication-exemption VLAN feature can be regarded as a kind of applications of secure channels.

- A maximum of 100 authentication-exemption VLANs can be configured.
- The authentication-exemption VLANs occupy hardware entries. When access control such as authentication is disabled, configuring authentication-exemption VLANs has the same effect as the case where no authentication-exemption VLANs are configured. Therefore, it is recommended that authentication-exemption VLANs be configured for users who need to access the Internet without authentication, only when the access control function has been enabled.
- Although packets from authentication-exemption VLANs are exempt from access control, they still need to be checked by a security ACL. If the packets of the users in an authentication-exemption VLAN are denied according to the security ACL, the users still cannot access the Internet.
- In gateway authentication mode, the device does not initiate any ARP request to a user in an authentication-exemption VLAN, and the ARP proxy will not work. Therefore, in gateway authentication mode, users in different authentication-exemption VLANs cannot access each other unless the users have been authenticated.

6.3.2 IPv4 User Capacity

To improve the operational stability of the device and guard against brutal force impacts from unauthorized users, you can restrict the total number of IPv4 access users on a certain port of the device.

Working Principle

If the total number of IPv4 access users is restricted, new users going beyond the total number cannot access the Internet.

Only the switches support the restriction on the number of IPv4 access users.

The number of IPv4 access users is not restricted on the device by default, but depends on the hardware capacity of the device.

The number of IPv4 access users includes the IPv4 authenticated users based on dot1x authentication, IPv4 users based on Web authentication, and IPv4 users based on various binding functions. Because the number of IPv4 access users is configured in interface configuration mode, the restriction includes both the number of IPv4 users generated on the port and IPv4 users globally generated. For example, you can set the maximum number of IPv4 access users on the Gi 0/1 port to 2, run commands to bind an IPv4 user to the port, and then run commands to bind a global IPv4 user to the port. Actually there are already two access users on the port. If you attempt to bind another IPv4 user or another global IPv4 user to the port, the binding operation fails.

6.3.3 Authenticated-User Migration

On an actual network, users do not necessarily access the Internet from a fixed place. Instead, users may be transferred to another department or office after getting authenticated at one place. They do not actively get offline but remove network cables and carry their mobile terminals to the new office to access the network. Then this brings about an issue about authenticated-user migration. If authenticated-user migration is not configured, a user who gets online at one place cannot get online at another place without getting offline first.

Working Principle

When authenticated-user migration is enabled, the dot1x or Web authentication module of the device detects that the port number or VLAN corresponding to a user's MAC address has changed. Then the user is forced offline and needs to be authenticated again before getting online.

Only the switches or wireless devices support authenticated-user migration. In addition, cross-switch migration is not supported. For example, authentication and migration are enabled on two N18000, and a user gets online after being authenticated on one of the two N18000. If the user attempts to migrate to the other N18000, the migration fails.

The authenticated-user migration function requires a check of users' MAC addresses, and is invalid for users who have IP addresses only.

The authenticated-user migration function enables a user who gets online at one place to get online at another place without getting offline first. If the user gets online at one place and then gets offline at that place, or if the user does not get online before moving to another place, the situation is beyond the control range of authenticated-user migration.

During migration, the system checks whether the VLAN ID or port number that corresponds to a user's MAC address has changed, so as to determine whether the user has migrated. If the VLAN ID or port number is the same, it indicates that the user does not migrate; otherwise, it indicates that the user has migrated. According to the preceding principle, if another user on the network uses the MAC address of an online user, the system will wrongly disconnect the online user unless extra judgment is made. To prevent such a problem, the dot1x or Web authentication will check whether a user has actually migrated. For a user who gets online through Web authentication or dot1x authentication with IP

authorization, the dot1x or Web authentication sends an ARP request to the original place 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, it indicates that the user's location has indeed changed and then the migration is allowed. If a response is received within the specified time, it indicates that the user actually does not migrate and a fraudulent user may exist on the network. In the latter case, the migration is not performed. The ARP request is sent once every second by default, and sent for a total of five times. This means that the migration cannot be confirmed until five seconds later. Timeout-related parameters, including the probe interval and probe times, can be changed using the **arp retry** times *times* and **arp retry** interval *interval* commands. For details about the specific configuration, see *ARP-SCG.doc*. It should be noted that the migration check requires the configuration of IP authorization for users based on dot1x authentication. In addition, the ARP probe is triggered only for user migration in gateway authentication mode but not triggered for user migration in access authentication mode.

6.3.4 User Online-Status Detection

After a user accesses the Internet, the user may forget to get offline or cannot actively get offline due to terminal faults. In this case, the user will keep being charged and therefore will suffer a certain economical loss. To protect the benefits of users on the Internet, the device provides a function to detect whether the users are really online. If the device considers that a user is not online, the device actively disconnects the user.

Working Principle

A specific detection interval is preset on the device. If a user's traffic is lower than a certain value in this interval, the device considers that the user is not using the network and therefore directly disconnects the user.

- Only the switches devices support the user online-status detection function.
- The user online-status detection function applies to only users who get online through dot1x or Web authentication.
- Currently, the N18000 supports zero-traffic detection only.
- Currently, due to hardware chip restrictions of the N18000, the time to disconnect a user without any traffic relates to the configured MAC address aging time. If the traffic detection interval is set to m minutes and the MAC address aging time is set to n minutes, the interval from the moment when an authenticated user leaves the network without actively getting offline to the moment when the user is disconnected upon detection of zero traffic is about [m, m+n] minutes. In other words, if an online user does not incur any Internet access traffic, the user is disconnected about [m, m+n] minutes later.
- Only one policy can be applied to one user group.

6.4 Configuration

Configuration Item	Suggestions and Related Commands	
Configuring Authentication-Exemption VLANs	Optional configuration, which is used to specify the users of which VLANs can access the Internet without authentication.	
	[no] direct-vlan	Configures authentication-exemption VLANs.
Configuring the IPv4 User Capacity	Optional configuration, which is used to specify the maximum number of users who are allowed to access a certain interface.	
	[no] nac-author-user maximum	Configures the number of IPv4 users who are allowed to access a certain interface.
Configuring Authenticated-User Migration	Optional configuration, which is used to specify whether online users with static MAC addresses can migrate.	
	[no] station-move permit	Configures whether authenticated users can migrate.
Configuring User Online-Status Detection	Optional configuration, which is used to specify whether to enable the user online-status detection function.	
	offline-detect interval threshold	Configures the parameters of the user online-status detection function.
	no offline-detect	Disables the user online-status detection function.
	default offline-detect	Restores the default user online-status detection mode.

6.4.1 Configuring Authentication-Exemption VLANs

Configuration Effect

Configure authentication-exemption VLANs, so that users in these VLANs can access the Internet without experiencing dot1x or Web authentication.

Configure authentication-exemption VLANs on a port, so that only users in specified VLANs on the port can access the Internet without experiencing authentication.

Precautions

Authentication-exemption VLANs only mean that users in these VLANs do not need to experience a check related to access authentication, but still need to experience a check based on a security ACL. If specified users or VLANs are denied according to the security ACL, corresponding users still cannot access the Internet. Therefore, during ACL configuration, you

need to ensure that specified VLANs or specified users in the authentication-exemption VLANs are not blocked if you hope that users in the authentication-exemption VLANs can access the Internet without being authenticated.

Configuration Method

Configuring Authentication-Exemption VLANs

- Optional configuration. To spare all users in certain VLANs from dot1x or Web authentication, configure these VLANS as authentication-exemption VLANs.
- Perform this configuration on access, convergence, or core switches depending on user distribution.
- Authentication-exemption VLANs can be configured in interface configuration mode.

Command	**[no] direct-vlan** *vlanlist*
Parameter Description	**no**: If the command carries this parameter, it indicates that the authentication-exemption VLAN configuration will be deleted. *vlanlist*: This parameter indicates the list of authentication-exemption VLANs to be configured or deleted.
Defaults	No authentication-exemption VLAN has been configured.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure or delete authentication-exemption VLANs.

Verification

Check the authentication-exemption VLAN configuration using the following method:

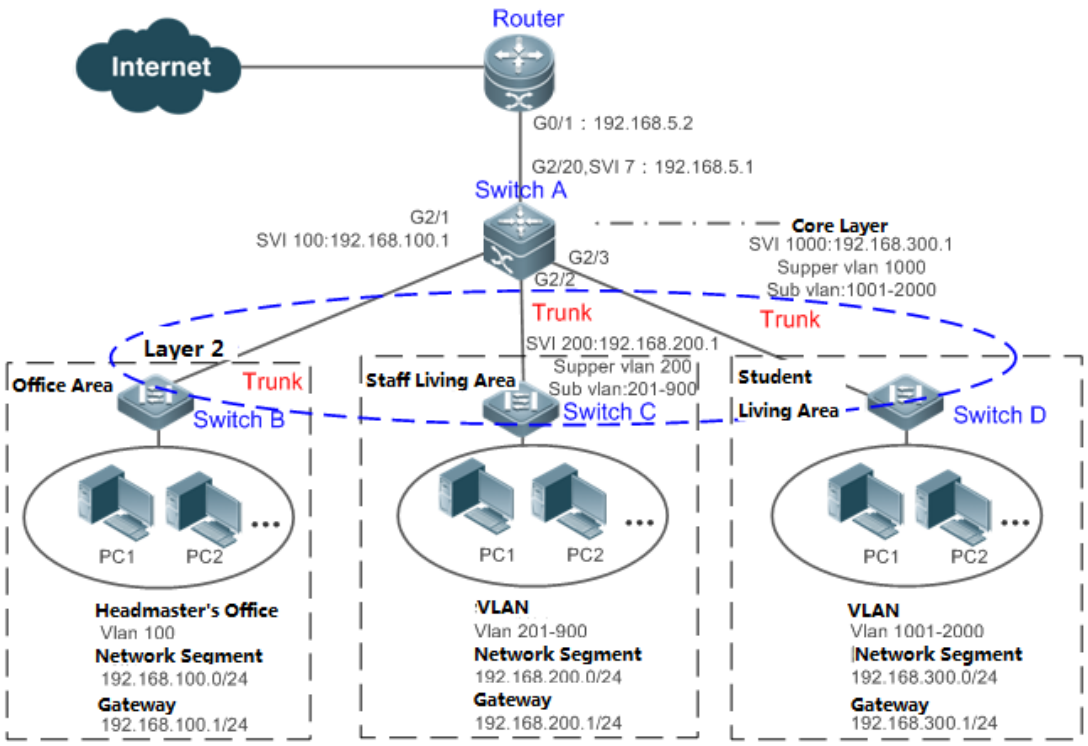
- Enable dot1x authentication on downlink ports that connect to user terminals, add the downlink ports that connect to the user terminals to a specific VLAN, and configure the VLAN as an authentication-exemption VLAN. Then open the Internet Explorer, and enter a valid extranet address (such as www.google.com). If the users can open the corresponding webpage on the Internet, it indicates that the authentication-exemption VLAN is valid; otherwise, the authentication-exemption VLAN does not take effect.
- Use the **show direct-vlan** command to check the authentication-exemption VLAN configuration on the device.

Command	**show direct-vlan**
Parameter Description	-
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode
Usage Example	`Hostname#show direct-vlan` `direct-vlan 100`

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring Authentication-exemption VLANs so that Specific Users Can Access the Internet Without Being Authenticated

Scenario **Figure 6-2**	
Configuration Steps	● On switch A (which is the core gateway device), set the GI 2/1 port as a trunk port, and enable dot1x authentication on this port. ● On switch A (which is the core gateway device), configure VLAN 100 to which the headmaster's office belongs as an authentication-exemption VLAN.

Switch A	`SwitchA(config)#vlan 100`
	`SwitchA(config-vlan)#exit`
	`SwitchA(config)#direct-vlan 100`
	`SwitchA(config)#int GigabitEthernet 0/1`
	`SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk`
	`SwitchA(config-if-GigabitEthernet 0/1)#dot1x port-control auto`
	`*Oct 17 16:06:45: %DOT1X-6-ENABLE_DOT1X: Able to receive EAPOL packet and DOT1X authentication enabled.`

Verification	● Open the Internet Explorer from any PC in the headmaster's office, enter a valid extranet address, and confirm that the corresponding webpage can be opened. ● Use the **show direct-vlan** command to check whether the authentication-exemption VLAN is valid.

Switch A	SwitchA(config)#show direct-vlan direct-vlan 100

6.4.2 Configuring the IPv4 User Capacity

Configuration Effect

Configure the IPv4 user capacity, so as to restrict the number of users who are allowed to access an access port.

Precautions

N/A

Configuration Method

Configuring the IPv4 User Capacity

- Optional configuration. To limit the maximum of users who are allowed to access an access port, configure the IPv4 user capacity. The access user capacity is not limited on an access port by default. Suppose the user capacity limit is configured on a specific interface. When the number of authenticated users on the interface reaches the maximum, new users cannot be authenticated on this interface and cannot get online, until existing authenticated users get offline on the interface.
- Perform this configuration on access switches, which may be access switches on the network edge or core gateway devices.

Command	**nac-author-user maximum** *max-user-num* **no nac-author-user maximum**
Parameter Description	**no**: If the command carries this parameter, it indicates that the limit on the IPv4 access user capacity will be removed from the port. *max-user-num*: This parameter indicates the maximum number of IPv4 users who allowed to access the port. The value range is from 1 to 1024.
Defaults	The number of IPv4 access users is not limited.
Command Mode	Interface configuration mode
Usage Guide	Use this command to limit the number of IPv4 access users on a specific access port.

Verification

Check the IPv4 user capacity configuration on a port using the following method:

- dot1x authentication: When the number of users who get online based on 1x client authentication on the port reaches the specified user capacity, no any new user can get online from this port.
- Web authentication: When the number of users who get online based on Web authentication on the port reaches the specified user capacity, no any new user can get online from this port.

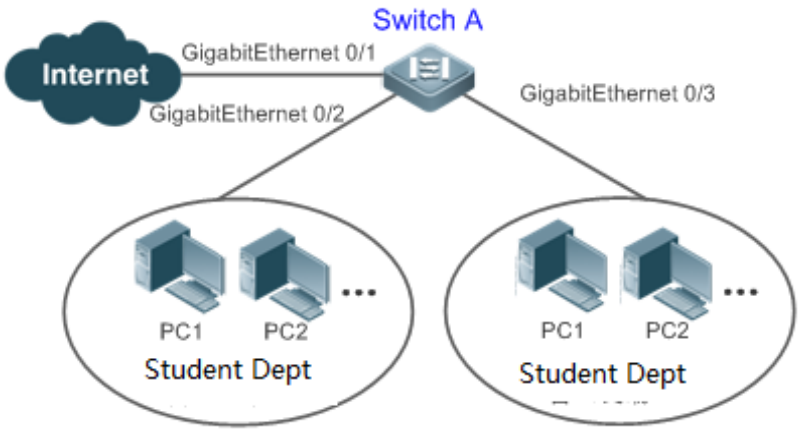
- Use the **show nac-author-user** [**interface** *interface-name*] command to check the IPv4 user capacity configured on the device.

Command	**show nac-author-user** [**interface** *interface-name*]
Parameter Description	***interface-name***: This parameter indicates the interface name.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Global configuration mode
Usage Example	Hostname#show nac-author-user interface GigabitEthernet 0/1 Port Cur_num Max_num -------- ------- ------- Gi0/1 0 4

Configuration Examples

The following configuration example describes SCC-related configuration only.

Restricting the Number of IP4 Users on a Port to Prevent Excessive Access Terminals from Impacting the Network

Scenario Figure 6-3	
Configuration Steps	● Assume that the dot1x authentication environment has been well configured on the access switch A, and dot1x authentication is enabled on the Gi 0/2 port. ● Set the maximum number of IPv4 access users on the Gi 0/2 port to 4.
Switch A	SwitchA(config)#int GigabitEthernet 0/2 SwitchA(config-if-GigabitEthernet 0/2)#nac-author-user maximum 4
Verification	● Perform dot1x authentication for all the four PCs in the dormitory, so that the PCs get online. Then take an additional terminal to access the network, and attempt to perform dot1x authentication for this terminal. Verify that the terminal cannot be successfully authenticated to get online.

	● Use the **show nac-author-user** command to check whether the configuration has taken effect.
Switch A	SwitchA(config)#show nac-author-user Port Cur_num Max_num -------- ------- ------- Gi0/1 0 4

6.4.3 Configuring Authenticated-User Migration

Configuration Effect

By default, when a user gets online after passing dot1x or Web authentication at a physical location (which is represented by a specific access port plus the VLAN number) and quickly moves to another physical location without getting offline, the user cannot get online through dot1x or Web authentication from the new physical location, unless the authenticated-user migration feature has been configured in advance.

Precautions

- If the authenticated-user migration feature is not yet configured, an online user cannot get online from the new physical location after quickly moving from one physical location to another physical location without getting offline first. However, if the user gets offline before changing the physical location or gets offline during the location change (for example, the user online-status detection function disconnects the user), the user can still normally get online after being authenticated at the new physical location, even if the authenticated-user migration feature is not configured.
- After moving to the new physical location, the online user needs to perform dot1x or Web authentication so as to get online.

Configuration Method

↘ Configuring Authenticated-User Migration

- Optional configuration. To allow users to be authenticated and get online from different physical locations, enable the authenticated-user migration function.
- Perform this configuration on access, convergence, or core switches depending on user distribution.

Command	**[no] station-move permit**
Parameter Description	**no station-move permit**: Indicates that authenticated-user migration is not permitted. **station-move permit**: Indicates that authenticated-user migration is permitted.
Defaults	Authenticated-user migration is not permitted; that is, when a user getting online from one physical location on the network moves to another physical location and attempts to get online from the new physical location without getting offline first, the authentication fails and the user cannot get online from the new physical location.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure authenticated-user migration.

Verification

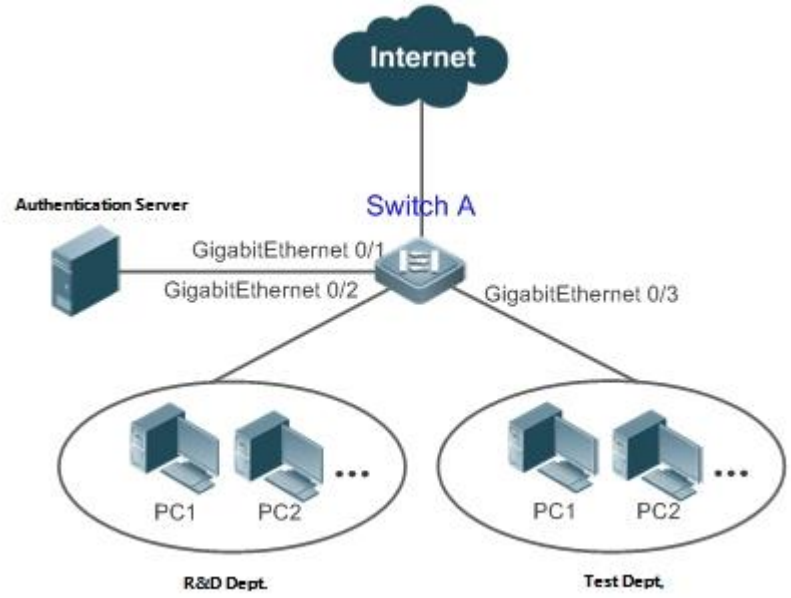
Check the authenticated-user migration configuration using the following method:

- A PC is authenticated and gets online from a dot1x-based port of the device using dot1x SU client, and does not actively get offline. Move the PC to another port of the device on which dot1x authentication is enabled, and perform dot1x authentication again. Check whether the PC can successfully get online.

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring Online-User Migration so that an Online User Can Perform Authentication and Get Online from Different Ports Without Getting Offline First

Scenario **Figure 6-4**	
Configuration Steps	● Enable dot1x authentication on access ports Gi 0/2 and Gi 0/3, and configure authentication parameters. The authentication is MAC-based. ● Configure online-user migration.
Switch A	`sw1(config)#station-move permit`
Verification	● A lap-top PC in the R&D department performs authentication using dot1x SU client, and gets online. Remove the network cable from the PC, connect the PC to the LAN where the test department resides, and perform dot1x authentication for the PC again using dot1x SU client. Confirm that the PC can successfully get online.
Switch A	`sw1(config)#show running-config | include station`

	station-move permit

6.4.4 Configuring User Online-Status Detection

Configuration Effect

After the user online-status detection function is enabled, if a user's traffic is lower than a certain threshold within the specified period of time, the device automatically disconnects the user, so as to avoid the economical loss incurred by constant charging to the user.

Precautions

It should be noted that if disconnecting zero-traffic users is configured, generally software such as 360 Security Guard will run on a user terminal by default. Then such software will send packets time and again, and the device will disconnect the user only when the user's terminal is powered off.

Configuration Method

Configuring User Online-Status Detection

- Optional configuration. A user is disconnected if the user does not involve any traffic within eight hours by default.
- Perform this configuration on access, convergence, or core switches depending on user distribution. The configuration acts on only the configured device instead of other devices on the network.
- If the traffic threshold parameter threshold is set to 0, it indicates that zero-traffic detection will be performed.

Command	**offline-detect interval** *interval* **threshold** *threshold* **no offline-detect** **default offline-detect**
Parameter Description	*interval*: This parameter indicates the offline-detection interval. The value range is from 6 to 65535 in minutes on a switch or from 1 to 65535 in minutes on a non-switch device. The default value is 8 hours, that is, 480 minutes. *threshold*: This parameter indicates the traffic threshold. The value range is from 0 to 4294967294 in bytes. The default value is 0, indicating that the user is disconnected when no traffic of the user is detected. **no offline-detect**: Disables the user online-status detection function. **default offline-detect**: Restores the default value. In other words, an online user will be disconnected when the device detects that the user does not have any traffic within eight hours.
Defaults	8 hours
Command Mode	Global configuration mode
Usage Guide	Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specific threshold within a specific period of time. Use the **no offline-detect** command to disable the user online-status detection function, or use the **default offline-detect** command to restore the default detection mode.

Verification

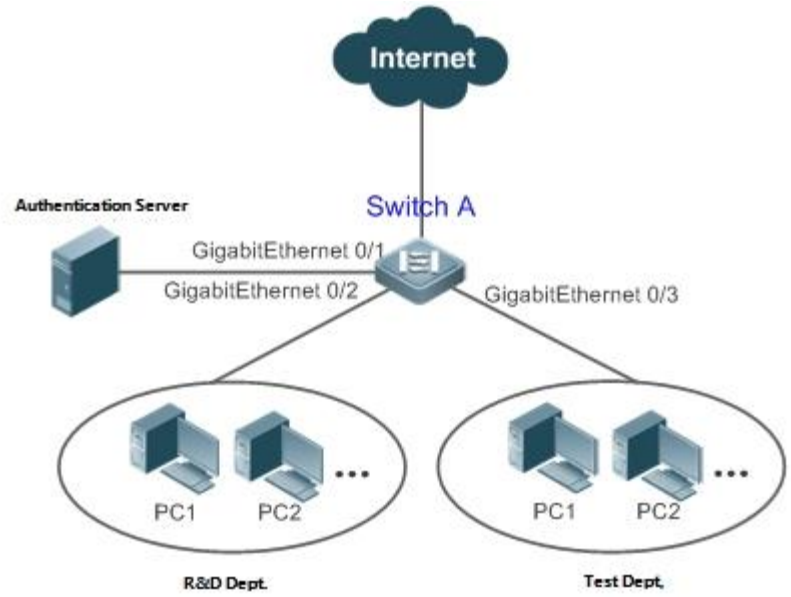
Check the user online-status detection configuration using the following method:

- After the user online-status detection function is enabled, power off the specified authenticated terminal after the corresponding user gets online. Then wait for the specified period of time, and run the online user query command associated with dot1x or Web authentication on the device to confirm that the user is already offline.

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring User Online-Status Detection so that a User Is Disconnected if the User Does Not Have Traffic Within Five Minutes

Scenario **Figure 6-5**	
Configuration Steps	• Enable dot1x authentication on the access port Gi 0/2, and configure authentication parameters. The authentication is MAC-based. • Configure user online-status detection so that a user is disconnected if the user does not have traffic within five minutes.
Switch A	`sw1(config)# offline-detect interval 5 threshold 0`
Verification	• Perform dot1x authentication using dot1x SU client for a PC in the R&D department, so that the PC gets online. Then power off the PC, wait for 6 minutes, and run the online user query command available with dot1x authentication on switch 1 to confirm that the user of the PC is already offline.
Switch A	`sw1(config)#show running-config | include offline-detect`

	offline-detect interval 5

6.5 Monitoring

Displaying

Command	Function
show direct-vlan	Displays the authentication-exemption VLAN configuration.
show nac-author-user [**interface** *interface-name*]	Displays information about IPv4 user entries on a specific interface.

Debugging

System resources are occupied when debugging information is output. Therefore, close the debugging switch immediately after use.

Command	Function
debug scc event	Debugs the SCC running process.
debug scc user [mac | author | mac]	Debugs SCC user entries.
debug scc acl-show summary	Debugs ACLs stored in the current SCC and delivered by various services.
debug scc acl-show all	Debugs all ALCs stored in the current SCC.

7 Configuring Global IP-MAC Binding

7.1 Overview

Enable the global IP-MAC binding function manually to verify the 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 bounding feature is used to verify the input packets. Note that the address binding feature takes precedence over the 802.1X authentication and port security.

7.2 Applications

Application	Description
Global IP-MAC Binding	Only hosts with the specified IP addresses can access the network, and the hosts connected to a device can move freely.

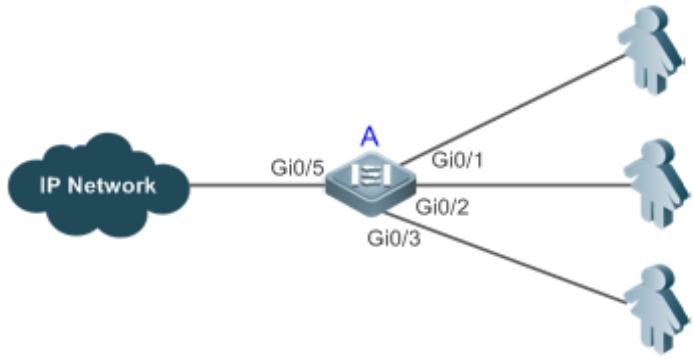
7.2.1 Global IP-MAC Binding

Scenario

The administrator assigns a fixed IP address for each host to facilitate management.

- Only hosts with the specified IP addresses can access the external network, which prevents IP address embezzlement by unauthorized hosts.
- Hosts can move freely under the same device.

Figure 7-1



Remarks	A is an access device. A user is a host configured with a static IP address.

	IP Network is an external IP network.

Deployment

- Manually configure the global IP-MAC binding. (Take three users as an example.)

User	MAC Address	IP Address
User 1	00d0.3232.0001	192.168.1.10
User 2	00d0.3232.0002	192.168.1.20
User 3	00d0.3232.0003	192.168.1.30

- Enable the IP-MAC binding function globally.
- Configure the uplink port (Gi0/5 port in this example) of the device as the exclude port.

7.3 Features

Basic Concepts

IPv6 Address Binding Mode

IPv6 address binding modes include Compatible, Loose, and Strict. The default mode is Strict. If IPv4-MAC binding is not configured, the IPv6 address binding mode does not take effect, and all IPv4 and IPv6 packets are allowed to pass through. If IPv4-MAC binding is configured, the IPv6 address binding mode takes effect, and the device forwards IPv4 and IPv6 packets based on the forwarding rules described in the following table:

Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the IPv4-MAC binding are forwarded.	Packets matching the IPv6-MAC binding are forwarded.
Loose	Packets matching the IPv4-MAC binding are forwarded.	If IPv6+MAC address binding is configured, packets matching the IPv6-MAC binding are forwarded. If IPv6-MAC binding does not exist, all IPv6 packets are forwarded.
Compatible	Packets matching the IPv4-MAC binding are forwarded.	If the IPv6 packets contain a MAC address matching the MAC address in the IPv4-MAC binding, the IPv6 packets are forwarded. Packets matching the IPv6-MAC binding conditions are forwarded.

The IPv4-MAC binding described in the preceding table can be generated by the global IP-MAC binding, or by other access security functions, such as port security and IP source guard. The IPv6-MAC binding can be generated in the same way.

Exclude Port

By default, the IP-MAC binding function takes effect on all ports of the device. You can configure exclude ports so that the address binding function does not take effect on these ports. In practice, the IP-MAC bindings of the input packets on the

uplink port are not fixed. Generally, the uplink port of the device is configured as the exclude port so that the packets on the uplink port are not checked for IP-MAC binding.

Overview

Feature	Description
Configuring Global IP-MAC Binding	Control forwarding of IPv4 or IPv6 packets.
Configuring the IPv6 Address Binding Mode	Change the IPv6 packet forwarding rules.
Configuring the Exclude Port	Disable the global address binding function on the specified port.

7.3.1 Configuring Global IP-MAC Binding

Working Principle

Enable the global IP-MAC binding function manually to verify the 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.

Related Configuration

Configuring IP-MAC Binding

Run the **address-bind** command in global configuration mode to add or delete an IPv4-MAC binding.

Enabling the IP-MAC Binding Function

Run the **address-bind install** command in global configuration mode to enable the IP-MAC binding function. By default, this function is disabled.

7.3.2 Configuring the IPv6 Address Binding Mode

Working Principle

After the IPv4-MAC binding is configured and the security function is enabled, IPv6 packets are forwarded based on the IPv6 address binding mode. IPv6 binding modes include Compatible, Loose, and Strict.

Related Configuration

Configuring the IPv6 Address Binding Mode

By default, the IPv6 address binding mode is Strict.

Run the **address-bind ipv6-mode** command to specify an IPv6 address binding mode.

7.3.3 Configuring the Exclude Port

Working Principle

Configure an exclude port so that the address binding function does not take effect on this port.

Related Configuration

Configuring the Exclude Port

Run the **address-bind uplink** command to configure an exclude port. By default, no port is the exclude port.

7.4 Configuration

Configuration	Description and Command	
Configuring Global IP-MAC Binding	(Mandatory) It is used to configure and enable address binding.	
	address-bind	Configures a global IPv4-MAC binding.
	address-bind install	Enables the address binding function.
	address-bind binding-filter logging	Configures a logging filter of global IPv4-MAC binding.
Configuring the IPv6 Address Binding Mode	(Optional) It is used to configure the IPv6 address binding mode.	
	address-bind ipv6-mode	Configures the IPv6 address binding mode.
Configuring the Exclude Port	(Optional) It is used to disable the address binding function on a specified port.	
	address-bind uplink	Configures an exclude port.

7.4.1 Configuring Global IP-MAC Binding

Configuration Effect

- Configure a global IPv4-MAC binding.
- Enable the address binding function to control forwarding of the IPv4 or IPv6 packets.

Notes

- If you run the **address-bind install** command without IP-MAC binding configured, IP-MAC binding does not take effect and all packets are allowed to pass through.

Configuration Steps

Configuring Global IP-MAC Binding

- (Mandatory) Perform this configuration in global configuration mode.

Enabling the Address Binding Function

- (Mandatory) Perform this configuration in global configuration mode.

Configuring a Logging Filter of Global IP-MAC Binding

- (Optional) Perform this configuration in global configuration mode.

Verification

Run the **show run** or **show address-bind** command to check whether the configuration takes effect.

Related Commands

Configuring Global IP-MAC Binding

Command	**address-bind** { *ip-address* | *ipv6-address* } *mac-address*
Parameter Description	*ip-address*: Indicates the bound IPv4 address. *ipv6-address*: Indicates the bound IPv6 address. *mac-address*: Indicates the bound MAC address.
Command Mode	Global configuration mode
Configuration Usage	Run this command to configure the binding relationship between an IPv4/IPv6 address and a MAC address.

Enabling the Address Binding Function

Command	**address-bind install**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	Run this command to enable the global IP-MAC binding function. This function is used to control forwarding of IPv4 or IPv6 packets.

Configuring a Logging Filter of Global IP-MAC Binding

Command	**address-bind binding-filter logging** [**rate-limit** *rate*]
Parameter Description	**rate-limit** *rate*: Indicates the printing rate of logging filter of global IPv4-MAC binding.
Command Mode	Global configuration mode
Configuration Usage	By default, the rate is 10 logs per minute. When a logging filter is configured, alert logs are printed if IP packets not containing matched IP address and MAC address are detected. When a logging filter is configured, the number of non-printed logs is prompted if the actual printing rate exceeds the set rate.

Configuration Example

Configuring Global IP-MAC Binding and Enabling Address Binding

Configuration Steps	● Configure a global IPv4-MAC binding. ● Enable the address binding function.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001 Hostname(config)# address-bind install
Verification	Display the global IP-MAC binding on the device.
	Hostname#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr --------------- ---------------- 192.168.5.1 00d0.f800.0001

7.4.2 Configuring the IPv6 Address Binding Mode

Configuration Effect

- Change the IPv6 address binding mode so as to change the forwarding rules for IPv6 packets.

Configuration Steps

Configuring the IPv6 Address Binding Mode

- (Optional) Perform this configuration when you want to change the forwarding rules for IPv6 packets.

Verification

- Run the **show run** command to check whether the configuration takes effect.

Related Commands

Configuring the IPv6 Address Binding Mode

Command	**address-bind ipv6-mode** { **compatible** | **loose** | **strict** }
Parameter Description	**compatible**: Indicates the Compatible mode. **loose**: Indicates the Loose mode. **strict**: Indicates the strict mode.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Configuring the IPv6 Address Binding Mode

Configuration Steps	● Configure a global IP-MAC binding. ● Enable the address binding function. ● Set the IPv6 address binding mode to Compatible.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001 Hostname(config)# address-bind install Hostname(config)# address-bind ipv6-mode compatible
Verification	Run the **show run** command to display the configuration on the device.

7.4.3 Configuring the Exclude Port

Configuration Effect

- The address binding function is disabled on the exclude port, and all IP packets can be forwarded.

Notes

- The configuration can be performed only on a switching port or an L2 aggregate port.

Configuration Steps

Configuring the Exclude Port

- (Optional) Perform this configuration in global configuration mode when you want to disable the address binding function on a specified port.

Verification

Run the **show run** or **show address-bind uplink** command to check whether the configuration takes effect.

Related Commands

Configuring the Exclude Port

Command Syntax	**address-bind uplink** *interface-id*
Parameter Description	*interface-id*: Indicates the ID of a switching port or an L2 aggregate port.
Command Mode	Global configuration mode

Configuration Usage	N/A

Configuration Example

Configuring the Exclude Port

Configuration Steps	● Create a global IPv4-MAC binding. ● Enable the address binding function. ● Configure an exclude port.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001 Hostname(config)# address-bind install Hostname(config)# address-bind uplink GigabitEthernet 0/1
Verification	Display the global IP-MAC binding on the device.
	Hostname#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr --- --- 192.168.5.1 00d0.f800.0001 Hostname#show address-bind uplink Port State --- --- Gi0/1 Enabled Default Disabled

7.5 Monitoring

Displaying

Description	Command
Displays the IP-MAC binding on the device.	**show address-bind**
Displays the exclude port.	**show address-bind uplink**

8 Configuring Password Policy

8.1 Overview

The Password Policy is a password security function provided for local authentication of the device. It is configured to control users' login passwords and login states.

The following sections introduce password policy only.

Protocols and Standards

N/A

8.2 Features

Basic Concepts

Minimum Password Length

Administrators can set a minimum length for user passwords according to system security requirements. If the password input by a user is shorter than the minimum password length, the system does not allow the user to set this password but displays a prompt, asking the user to specify another password of an appropriate length.

Strong Password Detection

The less complex a password is, the more likely it is to crack the password. For example, a password that is the same as the corresponding account or a simple password that contains only characters or digits may be easily cracked. For the sake of security, administrators can enable the strong password detection function to ensure that the passwords set by users are highly complex. After the strong password detection function is enabled, a prompt will be displayed for the following types of passwords:

1. Passwords that are the same as corresponding accounts;
2. Simple passwords that contain characters or digits only.

Mandatory Modification of Weak Passwords

By default, weak passwords are configurable. However, after this function is enabled, weak passwords have to be modified to strong ones, or the configuration fails. Weak passwords meet at least one of the following conditions:

1. Passwords that are the same as corresponding accounts;
2. Simple passwords that contain characters or digits only.

Password Life Cycle

The password life cycle defines the validity time of a user password. When the service time of a password exceeds the life cycle, the user needs to change the password.

If the user inputs a password that has already expired during login, the system will give a prompt, indicating that the password has expired and the user needs to reset the password. If the new password input during password resetting does not meet system requirements or the new passwords consecutively input twice are not the same, the system will ask the user to input the new password once again.

Guard Against Repeated Use of Passwords

When changing the password, the user will set a new password while the old password will be recorded as the user's history records. If the new password input by the user has been used previously, the system gives an error prompt and asks the user to specify another password.

The maximum number of password history records per user can be configured. When the number of password history records of a user is greater than the maximum number configured for this user, the new password history record will overwrite the user's oldest password history record.

Storage of Encrypted Passwords

Administrators can enable the storage of encrypted passwords for security consideration. When administrators run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If administrators disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

8.3 Configuration

Configuration	Description and Command	
Configuring the Password Security Policy	Optional configuration, which is used to configure a combination of parameters related to the password security policy.	
	password policy life-cycle	Configures the password life cycle.
	password policy min-size	Configures the minimum length of user passwords.
	password policy no-repeat-times	Sets the no-repeat times of latest password configuration, so that the passwords specified in these times of latest password configuration can no longer be used in future password configuration.
	password policy strong	Enables the strong password detection function.
	password policy forced-password-modify	Enables mandatory modification of weak passwords.
	service password-encryption	Sets the storage of encrypted passwords.

Networking Requirements

- Provide a password security policy for local authentication of the device. Users can configure different password security policies to implement password security management.

Notes

- The configured password security policy is valid for global passwords (configured using the commands **enable password** and **enable secret**) and local user passwords (configured using the **username** *name* **password** *password* command). It is invalid for passwords in Line mode.

Configuration Steps

Configuring the Password Life Cycle

- Optional
- Perform this configuration on each device that requires the configuration of a password life cycle unless otherwise stated.

Configuring the Minimum Length of User Passwords

- Optional
- Perform this configuration on each device that requires a limit on the minimum length of user passwords unless otherwise stated.

Setting the No-Repeat Times of Latest Password Configuration

- Optional
- Perform this configuration on each device that requires a limit on the no-repeat times of latest password configuration unless otherwise stated.

Enabling Mandatory Modification of Weak Passwords

- Optional
- Do not perform this configuration on each device unless otherwise stated.

Enabling the Strong Password Detection Function

- Optional
- Perform this configuration on each device that requires strong password detection unless otherwise stated.

Setting the Storage of Encrypted Passwords

- Optional
- Perform this configuration on each device that requires the storage of passwords in encrypted format unless otherwise stated.

Enabling the Check for Special Characters in a Password

- Optional
- If there is no special requirement, perform this configuration on each device that requires the check for special characters in a password.

Verification

Configure a local user on the device, and configure a valid password and an invalid password for the user.

- When you configure the valid password, the device correctly adds the password.
- When you configure the invalid password, the device displays a corresponding error log.

Related Commands

Configuring the Password Life Cycle

Command Syntax	**password policy life-cycle** *days*
Parameter Description	**life-cycle** *days*: Indicates the password life cycle in the unit of days. The value range is from 1 to 65535.
Command Mode	Global configuration mode
Usage Guide	The password life cycle is used to define the validity period of user passwords. If the user logs in with a password whose service time already exceeds the life cycle, a prompt is given, asking the user to change the password.

Configuring the Minimum Length of User Passwords

Command Syntax	**password policy min-size** *length*
Parameter Description	**min-size** *length*: Indicates the minimum length of passwords. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the minimum length of passwords. If the minimum length of passwords is not configured, users can input a password of any length.

Setting the No-Repeat Times of Latest Password Configuration

Command Syntax	**password policy no-repeat-times** *times*
Parameter Description	**no-repeat-times** *times*: Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.
Command Mode	Global configuration mode

Usage Guide	After this function is enabled, all old passwords used in the several times of latest password configuration will be recorded as the user's password history records. If the new password input by the user has been used previously, the system gives an error prompt and the password modification fails. You can configure the maximum number of password history records per user. When the number of password history records of a user is greater than the maximum number configured for the user, the new password history record will overwrite the user's oldest password history record.

Enabling Mandatory Modification of Weak Passwords

Command Syntax	**password policy forced-password-modify**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After mandatory modification of weak passwords is enabled, users have to change their passwords if the passwords are the same as corresponding accounts or contain characters or digits only.

Enabling the Strong Password Detection Function

Command Syntax	**password policy strong**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	After the strong password detection function is enabled, a prompt is displayed for the following types of passwords: 1. Passwords that are the same as corresponding accounts; 2. Simple passwords that contain characters or digits only.

Enabling the Check for Special Characters in a Password

Command Syntax	**password policy printable-character-check**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After strong password check and check for special characters in a password are configured, passwords that contain only special characters are invalid and cannot be configured successfully. There are 32 special characters in total, including 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 (/).

Setting the Storage of Encrypted Passwords

Command Syntax	**service password-encryption**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Before the storage of encrypted passwords is set, all passwords used in the configuration process will be displayed and stored in plaintext format, unless the passwords are configured in cipher text format. You can enable the storage of encrypted passwords for security consideration. When you run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If you disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

Checking User-Configured Password Security Policy Information

Command Syntax	**show password policy**
Parameter Description	-
Command Mode	Privileged EXEC mode/ Global configuration mode/ Interface configuration mode
Usage Guide	Use this command to display the password security policy configured on the device.

Checking Information Such as the Default Password Dictionary and Weak Passwords Manually Set

Command Syntax	**show password policy**
Parameter Description	-
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display information such as the default password dictionary and weak passwords manually set on the device.

Configuration Examples

The following configuration example describes configuration related to a password security policy.

Configuring Password Security Check on the Device

Typical Application	Assume that the following password security requirements arise in a network environment: 1. The minimum length of passwords is 8 characters; 2. The password life cycle is 90 days; 3. Passwords are stored and transmitted in cipher text format; 4. The number of no-repeat times of password history records is 3; 5. Passwords shall not be the same as user names, and shall not contain simple characters or digits only. 6. Mandatory modification of weak passwords is enabled.
Configuration Steps	● Set the minimum length of passwords to 8. ● Set the password life cycle to 90 days. ● Enable the storage of encrypted passwords. ● Set the no-repeat times of password history records to 3. ● Enable the strong password detection function. ● Enable mandatory modification of weak passwords.
	Hostname# configure terminal Hostname(config)# password policy min-size 8 Hostname(config)# password policy life-cycle 90 Hostname(config)# service password-encryption Hostname(config)# password policy no-repeat-times 3 Hostname(config)# password policy strong Hostname(config)# password policy forced-password-modify
Verification	When you create a user and the corresponding password after configuring the password security policy, the system will perform relevant detection according to the password security policy. ● Run the **show password policy** command to display user-configured password security policy information.
	Hostname# show password policy Global password policy configurations: Password encryption: Enabled Password strong-check: Enabled Password forced-password-modify Enabled Password secret-dictionary-check: Enabled Password min-size: Enabled (8 characters) Password life-cycle: Enabled (90 days) Password no-repeat-times: Enabled (max history record: 3)

Common Errors

- The time configured for giving a pre-warning notice about password expiry to the user is greater than the password life cycle.

8.4 Monitoring

Displaying

Command	Function
show password policy	Displays user-configured password security policy information.

9 Configuring Storm Control

9.1 Overview

When a local area network (LAN) has excess broadcast data flows, multicast data flows, 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 data flows, multicast data flows, or unknown unicast data flows. If the rate of data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds. This prevents flood data from entering the LAN causing a storm.

9.2 Applications

Application	Description
Network Attack Prevention	Enable storm control to prevent flooding.

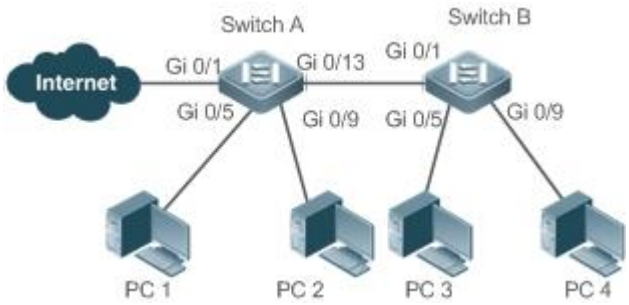
9.2.1 Network Attack Prevention

Scenario

The application requirements of network attack prevention are described as follows:

- Protect devices from flooding of broadcast packets, multicast packets, or unknown unicast packets.

Figure 9-1



Remarks	Switch A and Switch B are access devices. PC 1, PC 2, PC 3, and PC 4 are desktop computers.

Deployment

- Enable storm control on the ports of all access devices (Switch A and Switch B).

9.3 Features

Basic Concepts

Storm Control

If the rate of data flows (broadcast packets, multicast packets, or unknown unicast packets) received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

Storm Control Based on the Bandwidth Threshold

If the rate of data flows received by a device port is within the configured bandwidth threshold, the data flows are permitted to pass through. If the rate exceeds the threshold, excess data flows are discarded until the rate falls within the threshold.

Storm Control Based on the Packets-per-Second Threshold

If the rate of data flows received by a device port is within the configured packets-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the threshold, excess data flows are discarded until the rate falls within the threshold.

Storm Control Based on the Kilobits-per-Second Threshold

If the rate of data flows received by a device port is within the configured kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the threshold, excess data flows are discarded until the rate falls within the threshold.

Overview

Feature	Description
Unicast Packet Storm Control	Limits unknown unicast packets to prevent flooding.
Multicast Packet Storm Control	Limits multicast packets to prevent flooding.
Broadcast Packet Storm Control	Limits broadcast packets to prevent flooding.

9.3.1 Unicast Packet Storm Control

The unicast packet storm control feature monitors the rate of unknown unicast data flows received by a device port to limit LAN traffic and prevent flooding caused by excess data flows.

Working Principle

If the rate of unknown unicast data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

Related Configuration

↘ Enabling Unicast Packet Storm Control on Ports

By default, unicast packet storm control is disabled on ports.

Run the **storm-control unicast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }] command to enable unicast packet storm control on ports.

Run the **no storm-control unicast** or **default storm-control unicast** command to disable unicast packet storm control on ports.

The default command parameters are determined by related products.

9.3.2 Multicast Packet Storm Control

The multicast packet storm control feature monitors the rate of multicast data flows received by a device port to limit LAN traffic and prevent flooding caused by excess data flows.

Working Principle

If the rate of multicast data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

Related Configuration

↘ Enabling Multicast Packet Storm Control on Ports

By default, multicast packet storm control is disabled on ports.

Run the **storm-control multicast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }] command to enable multicast packet storm control on ports.

Run the **no storm-control multicast** or **default storm-control multicast** command to disable multicast packet storm control on ports.

The default command parameters are determined by related products.

9.3.3 Broadcast Packet Storm Control

The broadcast packet storm control feature monitors the rate of broadcast data flows received by a device port to limit LAN traffic and prevent flooding caused by excess data flows.

Working Principle

If the rate of broadcast data flows received by a device port is within the configured bandwidth threshold, packets-per-second threshold, or kilobits-per-second threshold, the data flows are permitted to pass through. If the rate exceeds the thresholds, excess data flows are discarded until the rate falls within the thresholds.

Related Configuration

Enabling Broadcast Packet Storm Control on Ports

By default, broadcast packet storm control is disabled on ports.

Run the **storm-control broadcast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }] command to enable broadcast packet storm control on ports.

Run the **no storm-control broadcast** or **default storm-control broadcast** command to disable broadcast packet storm control on ports.

9.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of Storm Control	(Mandatory) It is used to enable storm control.	
	storm-control { **broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*}]	Enables storm control.

9.4.1 Configuring Basic Functions of Storm Control

Configuration Effect

- Prevent flooding caused by excess broadcast packets, multicast packets, and unknown unicast packets.

Notes

- When you run a command (for example, **storm-control unicas**t) to enable storm control, if you do not set the parameters, the default values are used.

Configuration Steps

Enabling Unicast Packet Storm Control

- Mandatory.
- Enable unicast packet storm control on every device unless otherwise specified.

Enabling Multicast Packet Storm Control

- Mandatory.
- Enable multicast packet storm control on every device unless otherwise specified.

Enabling Broadcast Packet Storm Control

- Mandatory.
- Enable broadcast packet storm control on every device unless otherwise specified.

Verification

- Run the **show storm-control** command to check whether the configuration is successful.

Related Commands

Enabling Unicast Packet Storm Control

Command	**storm-control unicast** [{ **level** *percent* | **pps** *packets* | *rate-bps*}]
Parameter Description	**level** *percent*: Indicates the bandwidth percentage. **pps** *packets*: Indicates the number of packets per second. *rate-bps*: Indicates the packet rate.
Command Mode	Interface configuration mode
Usage Guide	Storm control can be enabled only on switch ports.

Enabling Multicast Packet Storm Control

Command	**storm-control multicast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }]
Parameter Description	**level** *percent*: Indicates the bandwidth percentage. **pps** *packets*: Indicates the number of packets per second. *rate-bps*: Indicates the packet rate.
Command Mode	Interface configuration mode
Usage Guide	Storm control can be enabled only on switch ports.

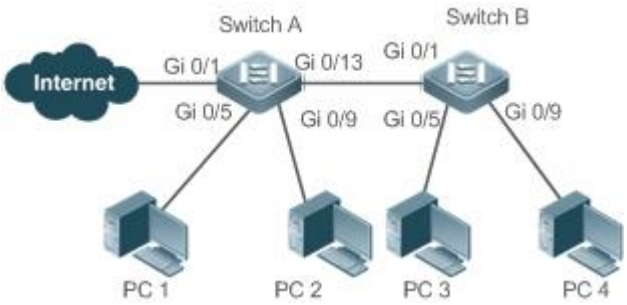
Enabling Broadcast Packet Storm Control

Command	**storm-control broadcast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }]
Parameter Description	**level** *percent*: Indicates the bandwidth percentage. **pps** *packets*: Indicates the number of packets per second. *rate-bps*: Indicates the packet rate.
Command Mode	Interface configuration mode
Usage Guide	Storm control can be enabled only on switch ports.

Configuration Example

Enabling Storm Control on Devices

Scenario	

Figure 9-2	
Configuration Step	● Enable storm control on Switch A and Switch B.

Switch A	`Hostname(config)#interface range gigabitEthernet 0/5,0/9,0/13`
	`Hostname(config-if-range)#storm-control broadcast`
	`Hostname(config-if-range)#storm-control multicast`
	`Hostname(config-if-range)#storm-control unicast`

Switch B	`Hostname(config)#interface range gigabitEthernet 0/1,0/5,0/9`
	`Hostname(config-if-range)#storm-control broadcast`
	`Hostname(config-if-range)#storm-control multicast`
	`Hostname(config-if-range)#storm-control unicast`

Verification	Check whether storm control is enabled on Switch A and Switch B.

Switch A	`Hostname# sho 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`

Switch B	`Hostname#sho 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

9.5 Monitoring

Displaying

Description	Command
Displays storm control information.	**show storm-control** [*interface-type interface-number*]

10 Configuring SSH

10.1 Overview

Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is encrypted. When a user in an insecure network environment logs into a device remotely, SSH helps ensure information security and powerful authentication, protecting the device against attacks such as IP address spoofing and plain-text password interception.

An SSH-capable device can be connected to multiple SSH clients. In addition, the device can also function as an SSH client, and allows users to set up an SSH connection with a SSH-server device. In this way, the local device can safely log in to a remote device through SSH to implement management.

- Currently, a device can work as either the SSH server or an SSH client, supporting SSHv1 and SSHv2 versions. Hostname SSH service supports both IPv4 and IPv6.
- Unless otherwise specified, SSH in this document refers to SSHv2.

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
- draft-ietf-secsh-filexfer-05: SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00: The version of the SSH Remote Login Protocol is 1.5. Comware implements the SSH server functions, but not the SSH client functions.

10.2 Applications

Application	Description
SSH Device Management	Use SSH to manage devices.
SSH Local Line Authentication	Use the local line password authentication for SSH user authentication.

Application	Description
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH user authentication.
SSH Public Key Authentication	Use the public key authentication for SSH user authentication.
SSH File Transfer	Use the Secure Copy (SCP) commands on the client to exchange data with the SSH server.
SSH Client Application	Use the SSH client to safely log in to a remote device for management.

10.2.1 SSH Device Management

Scenario

You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows system does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client. Figure 10-1 shows the network topology.

Figure 10-1 Networking Topology of SSH Device Management



Deployment

Configure the SSH client as follows:

- Start the PuTTY software.
- On the **Session** option tab of PuTTY, type in the host IP address of the SSH server and SSH port number **22**, and select the connection type **SSH**.
- On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**.
- On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**.
- Click **Open** to connect to the SSH server.
- Type in the correct user name and password to enter the terminal login interface.

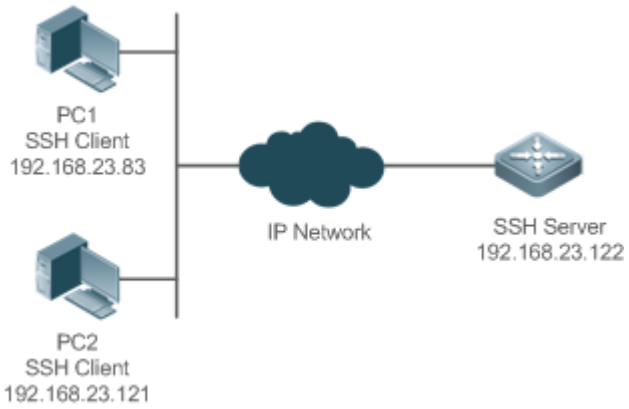
10.2.2 SSH Local Line Authentication

Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 10-2. To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server function is enabled. The requirements are as follows:

- SSH users use the local line password authentication mode.
- Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.

Figure 10-2 Networking Topology of SSH Local Line Password Authentication



Deployment

- Configure the SSH server as follows:

3. Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.
4. Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH clients, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 adopts an RSA or DSA key.
5. Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server using this IP address. The routes from the SSH clients to the SSH server are reachable.

- Configure the SSH client as follows:

Diversified SSH client software is available, including PuTTY,Linux, and OpenSSH. This document takes PuTTY as an example to explain the method for configuring the SSH clients.

4. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)
5. Set the IP address and connected port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22. Click **Open** to start the connection. As the current authentication mode does not require a user name, you can type in any user name, but cannot be null. (In this example, the user name is "anyname".)

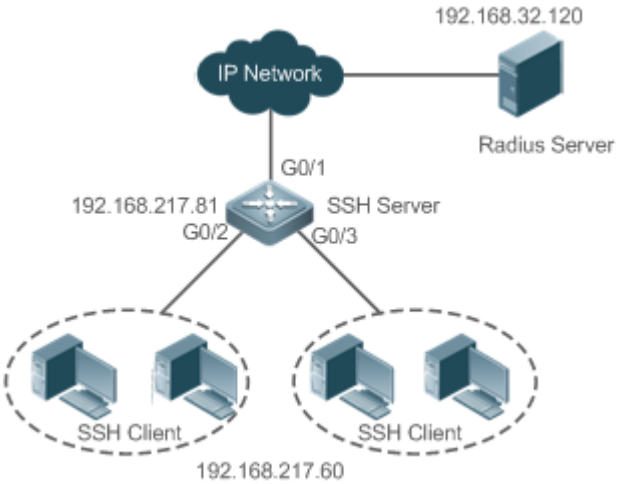
10.2.3 SSH AAA Authentication

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 10-3. To ensure security of data exchange, the PCs function as the SSH clients, and uses the SSH protocol to log in to the network device where the SSH

server is enabled. To better perform security management, the AAA authentication mode is used for user login on the SSH clients. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, it turns to the local authentication.

Figure 10-3 Networking Topology of SSH AAA Authentication



Deployment

- The routes from the SSH clients to the SSH server are reachable, and the route from the SSH server to the Radius server is also reachable.
- Configure the SSH server on the network device that functions as an SSH client.
- Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.

10.2.4 SSH Public Key Authentication

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 10-4.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 10-4 Network Topology for Public Key Authentication of SSH Users



Deployment

- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure the public key on the SSH server, and select the public key authentication mode.

- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash and associates the file with the SSH user name. Each user can be associated with one RSA public key and one DSA public key.

10.2.5 SSH Client Application

Scenario

The SSH service is enabled on a remote SSH server, and the **ssh** command is used on the local client to set up an SSH connection with the server for secure data transmission, as shown in Figure 10-5.

Figure 10-5 Networking Topology of SSH Client Application



Deployment

- Enable the SSH service on the server.
- On the client, run the **ssh** command to set up an SSH connection with the server for secure data transmission.

10.3 Features

Basic Concepts

User Authentication Mechanism

- Password authentication

During the password authentication, a client sends a user authentication request and encrypted user name and password to the server. The server decrypts the received information, compares the decrypted information with those stored on the server, and then returns a message indicating the successful or unsuccessful authentication.

- Public key authentication

During the public key authentication, digital signature algorithms, such as RSA and DSA, are used to authenticate a client. The client sends a public key authentication request to the server. This request contains information including the user name, public key, and public key algorithm. On receiving the request, the server checks whether the public key is correct. If wrong, the server directly sends an authentication failure message. If right, the server performs digital signature authentication on the client, and returns a message indicating the successful or unsuccessful authentication.

Public key authentication is applicable only to the SSHv2 clients.

SSH Communication

To ensure secure communication, interaction between an SSH server and an SSH client undergoes the following seven stages:

- Connection setup

The server listens on Port 22 to the connection request from the client. After originating a socket initial connection request, the client sets up a TCP socket connection with the server.

- Version negotiation

If the connection is set up successfully, the server sends a version negotiation packet to the client. On receiving the packet, the client analyzes the packet and returns a selected protocol version to the server. The server analyzes the received information to determine whether version negotiation is successful.

- Key exchange and algorithm negotiation

If version negotiation is successful, key exchange and the algorithm negotiation are performed. The server and the client exchange the algorithm negotiation packet with each other, and determine the final algorithm based on their capacity. In addition, the server and the client work together to generate a session key and a 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, the client sends an authentication request to the server. 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

After the successful authentication, the client sends a session request to the server. The server waits and processes the client request. After the session request is successfully processed, SSH enters the session interaction stage.

- Session interaction

After the session request is successfully processed, SSH enters the session interaction stage. Encrypted data can be transmitted and processed in both directions. The client sends a command to be executed to the client. The server decrypts, analyzes, and processes the received command, and then sends the encrypted execution result to the client. The client decrypts the execution result.

- Session ending

When the interaction between the server and the client is terminated, the socket connection disconnects, and the session ends.

Overview

Feature	Description
SSH Server	Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client.
SCP Service	After the SCP service is enabled, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

SSH Client	You can use the SSH client on the device to set up a secure connection with the SSH server on a network device.

10.3.1 SSH Server

Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client. You can also shut down the SSH server function to disconnect from all SSH clients.

Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts." In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

- Version: Configure the SSH version as SSHv1 orSSHv2 to connect SSH clients.
- Authentication timeout: The SSH server starts the timer after receiving a user connection request. The SSH server is disconnected from the client either when the authentication succeeds or when the authentication timeout is reached.
- Maximum number of authentication retries: The SSH server starts authenticating the client after receiving its connection request. If authentication does not succeed when the maximum number of user authentication retries is reached, a message is sent, indicating the authentication failure.
- Public key authentication: The public key algorithm can be RSA or DSA. It provides a secure connection between the client and the server. The public key file on the client is associated with the user name. In addition, the public key authentication mode is configured on the client, and the corresponding private key file is specified. In this way, when the client attempts to log in to the server, public key authentication can be implemented to set up a secure connection.

Related Configuration

Enabling the SSH Server

By default, the SSH server is disabled.

In global configuration mode, run the [**no**] **enable service ssh-server** command to enable or disable the SSH server.

To generate the SSH key, you also need to enable the SSH server.

Specifying the SSH Version

By default, the SSH server supports both SSHv1 and SSHv2, connecting either SSHv1 clients or SSHv2 clients.

Run the **ip ssh version** command to configure the SSH version supported by the SSH server.

If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

Run the **ip ssh time-out** command to configure the user authentication timeout of the SSH server. Use the **no** form of the command to restore the default timeout. The SSH server starts the timer after receiving a user connection request. If authentication does not succeed before the timeout is reached, authentication times out and fails.

Configuring the Maximum Number of SSH Authentication Retries

By default, the maximum number of user authentication retries is 3.

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user authentication retries. If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

Specifying the SSH Encryption Mode

By default, the encryption mode supported by the SSH server is Compatible, that is, supporting cipher block chaining (CBC), counter (CTR) and other encryption modes.

Run the **ip ssh cipher-mode** command to configure the encryption mode supported by the SSH server. Use the **no** form of the command to restore the default encryption mode supported by the SSH server.

Specifying the SSH Message Authentication Algorithm

By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5,SHA1, SHA1-96, and MD5-96, are supported.

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithm supported by the SSH server. Use the **no** form of the command to restore the default message authentication algorithm supported by the SSH server.

Setting A Monitoring Port ID for the SSH Server

The default port ID is 22.

Run the **ip ssh port** command to set a monitoring port ID for the SSH server. Use either the **no ip ssh port** command or the **ip ssh port 22** command to restore the default setting.

Enabling the Public Key Authentication on the SSH Server

Run the **ip ssh peer** command to associate the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Configuring the Minimum Length of the Key Generated by the Key Exchange Algorithm of the SSH Server

The default minimum length of the key generated by the key exchange algorithm of the SSH server is 2048 bytes.

Disabling the IP Address Blocking Function

Run the **ip ssh ip-block disable** command to disable the IP address blocking function on the SSH server.

Configuring the Diffie–Hellman (DH) Algorithm Supported by the SSH Server

By default, SSHv1 servers support no DH algorithm. SSHv2 servers support diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, and ecdh_sha2_nistp521.

10.3.2 SCP Service

The SSH server provides the SCP service to implement secure file transfer between the server and the client.

Working Principle

- SCP is a protocol that supports online file transfer. It runs on Port 22 based on the BSC RCP protocol, whereas RCP provides the encryption and authentication functions based on the SSH protocol. RCP implements file transfer, and SSH implements authentication and encryption.
- Assume that the SCP service is enabled on the server. When you use an SCP client to upload or download files, the SCP client first analyzes the command parameters, sets up a connection with a remote server, and starts another SCP process based on this connection. This process may run in source or sink mode. (The process running in source mode is the data provider. The process running in sink mode is the destination of data.) The process running in source mode reads and sends files to the peer end through the SSH connection. The process running in sink mode receives files through the SSH connection.

Related Configuration

Enabling the SCP Server

By default, the SCP server function is disabled.

Run the **ip scp server enable** command to enable SCP server function on a network device.

10.3.3 SSH Client

The SSH client is used to set up a secure connection with a remote network device on which the SSH server runs.

Working Principle

For details about the working principle of the SSH client, see the "SSH Communication" in "Basic Concepts."

Related Configuration

Specifying the Source Interface of the SSH Client

By default, the source address of SSH packets is searched based on the destination address.

Run the **ip ssh source-interface** *interface-name* command to specify the source interface of the SSH client.

Establishing a Session with the SSH Server

Run the **ssh** command to log in to a remote device that supports the SSH Server

Recovering an Established SSH Session

- Run the **ssh-session** *session-id* command to recover an established SSH session.

Disconnecting a Suspended SSH Session

- Run the **disconnect ssh-session** *session-id* command to disconnect a specified SSH session.

10.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.
	disconnect ssh[**vty**] *session-id*	Disconnects an established SSH session.
	crypto key generate {**rsa**|**dsa**}	Generates an SSH key.
	ip ssh version {**1**|**2**}	Specifies the SSH version.
	ip ssh time-out *time*	Configures the SSH authentication timeout.
	ip ssh authentication-retries *retry times*	Configures the maximum number of SSH authentication retries.
	Ip ssh cipher-mode{**cbc** | **ctr** | **others** }	Specifies the SSH encryption mode.
	Ip ssh hmac-algorithm{**md5** | **md5-96** | **sha1** | **sha1-96 | sha2-256 | sha2-512** }	Specifies the SSH message authentication algorithm.
	ip ssh port *port*	Sets a monitoring port ID for the SSH server.
	ip ssh peer *test* **public-key rsa flash** *:rsa.pub*	Associates an RSA public key file with a user.
	ip ssh peer *test* **public-key dsa flash***:dsa.pub*	Associates a DSA public key file with a user.
Configuring the SCP Service	Mandatory.	
	ip scp server enable	Enables the SCP server.
Configuring the SSH Client	(Optional)It is used to set up a secure connection with a remote network device that supports the SSH server.	
	ip ssh source-interface *interface-name*	Specifies the source interface of the SSH client.
	ssh [**oob**] [**-v** {**1** | **2** }][**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*] [**-m** {**hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }] [**-p** *port-num*] { *ip-addr*| *hostname*} [**/source** {**ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name*}] [**/vrf** *vrf-name*]	Establishes an encrypted session with a remote network device.

10.4.1 Configuring the SSH Server

Configuration Effect

- Enable the SSH server function on a network device so that you can set up a secure connection with a remote network device through the SSH client. All interactive data is encrypted before transmitted, featuring authentication and security.
- You can use diversified SSH user authentications modes, including local line password authentication, AAA authentication, and public key authentication.
- You can generate or delete an SSH key.
- You can specify the SSH version.
- You can configure the SSH authentication timeout.
- You can configure the maximum number of SSH authentication retries.
- You can specify the SSH encryption mode.
- You can specify the SSH message authentication algorithm.
- You can specify ACL filtering of the SSH server.

Notes

- The precondition of configuring a device as the SSH server is that communication is smooth on the network that the device resides, and the administrator can access the device management interface to configure related parameters.
- The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key.
- The SSH module does not support hot standby. Therefore, for products that supports hot standby on the supervisor modules, if no SSH key file exist on the new active module after failover, you must run the **crypto key generate** command to re-generate a key before using SSH.

Configuration Steps

↘ Enabling the SSH Server

- Mandatory.
- By default, the SSH server is disabled. In global configuration mode, enable the SSH server and generate an SSH key so that the SSH server state changes to ENABLE.

↘ Specifying the SSH Version

- Optional.
- By default, the SSH server supports SSHv1 and SSHv2, connecting either SSHv1 or SSHv2clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

↘ Configuring the SSH Authentication Timeout

- Optional.

- By default, the SSH authentication timeout is 120s. You can configure the user authentication timeout as required. The value ranges from 1 to 120. The unit is second.

Configuring the Maximum Number of SSH Authentication Retries

- Optional.
- Configure the maximum number of SSH authentication retries to prevent illegal behaviors such as malicious guessing. By default, the maximum number of SSH authentication retries is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum number of retries as required. The value ranges from 0 to 5.

Specifying the SSH Encryption Mode

- Optional.
- Specify the encryption mode supported by the SSH server. By default, the encryption mode supported by the SSH server is Compatible, that is, supporting CBC, CTR and other encryption modes.

Specifying the SSH Message Authentication Algorithm

- Optional.
- Specify the message authentication algorithm supported by the SSH server. By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5, SHA1, SHA1-96, and MD5-96, are supported.

Setting ACL Filtering of the SSH Server

- Optional.
- Set ACL filtering of the SSH server. By default, ACL filtering is not performed for all connections to the SSH server. According to needs, set ACL filtering to perform for all connections to the SSH server.

Enabling the Public Key Authentication for SSH Users

- Optional.
- Only SSHv2 supports authentication based on the public key. This configuration associates a public key file on the client with a user name. When a client is authenticated upon login, a public key file is specified based on the user name.

Enabling the SSHv1 Function

- Optional.
- You must enable the SSHv1 function to use SSHv1.

Configuring the Minimum Length of the Key Generated by the Key Exchange Algorithm of the SSH Server

- Optional.

Enabling the IP Address Blocking Function on the SSH Server

- Optional.

Configuring the Number of Authentication Failures for Blocking IP Addresses and the Time Period for Counting Authentication Failures on the SSH Server

- Optional.

Configuring the Time Period for Unblocking Blocked IP Addresses on the SSH Server

- Optional.

Configuring the Diffie–Hellman (DH) Algorithm Supported by the SSH Server

- Optional.

Verification

- Run the **show ip ssh** command to display the current SSH version, authentication timeout, and maximum number of authentication retries of the SSH server.
- Run the **show crypto key mypubkey** command to display the public information of the public key to verify whether the key has been generated.
- Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Related Commands

Enabling the SSH Server

Command	**enable service ssh-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To disable the SSH server, run the **no enable service ssh-server** command in global configuration mode. After this command is executed, the SSH server state changes to DISABLE.

Disconnecting an Established SSH Session

Command	**disconnect ssh**[**vty**] *session-id*
Parameter Description	**vty:** Indicates an established virtual teletype terminal (VTY) session. *session-id*: Indicates the ID of the established SSH session. The value ranges from 0 to 35.
Command Mode	Privileged EXEC mode
Usage Guide	Specify an SSH session ID to disconnect the established SSH session. Alternatively, specify a VTY session ID to disconnect a specified SSH session. Only an SSH session can be disconnected.

Generating an SSH Key

Command	**crypto key generate** {**rsa**|**dsa**}
Parameter Description	**rsa:** Generates an RSA key. **dsa:** Generates a DSA key.
Command Mode	Global configuration mode
Usage Guide	The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. If an RSA key is generated, both SSHv1 and SSHv2 are supported. If only a DSA key is generated, only SSHv2 can use the key.

Specifying the SSH Version

Command	**ip ssh version** {**1**|**2**}
Parameter Description	**1:** Indicates that the SSH server only receives the connection requests sent by SSHv1 clients. **2:** Indicates that the SSH server only receives the connection requests sent by SSHv2 clients.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh version** command to restore the default settings. By default, the SSH server supports both SSHv1 and SSHv2.

Configuring the SSH Authentication Timeout

Command	**ip ssh time-out** *time*
Parameter Description	*time*: Indicates the SSH authentication timeout. The value ranges from 1 to 120. The unit is second.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh time-out** command to restore the default SSH authentication timeout, which is 120s.

Configuring the Maximum Number of SSH Authentication Retries

Command	**ip ssh authentication-retries** *retry times*
Parameter Description	*retry times*: Indicates the maximum number of user authentication retries. The value ranges from 0 to 5.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh authentication-retries** command to restore the default number of user authentication retries, which is 3.

Specifying the SSH Encryption Mode

Command	**ip ssh cipher-mode**{**cbc** | **ctr** | **others** }
Parameter	**cbc:** Sets the encryption mode supported by the SSH server to the CBC mode. Corresponding algorithms

Description	include DES-CBC,3DES-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC, and Blowfish-CBC. **ctr:** Sets the encryption mode supported by the SSH server to the CTR mode. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR. **others:** Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is RC4.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the encryption mode supported by the SSH server. On devices, the SSHv1 server supports the DES-CBC, 3DES-CBC, and Blowfish-CBC encryption algorithms; the SSHv2 server supports the AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4 encryption algorithms. These algorithms can be grouped into three encryption modes: CBC, CTR, and others. As the cryptography continuously develops, it is approved that encryption algorithms in the CBC and others modes can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption mode supported by the SSH server to CTR to increase the security level of the SSH server.

Specifying the SSH Message Authentication Algorithm

Command	**ip ssh hmac-algorithm**{**md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }
Parameter Description	**md5:** Indicates that the message authentication algorithm supported by the SSH server is MD5. **md5-96:** Indicates that the message authentication algorithm supported by the SSH server is MD5-96. **sha1:** Indicates that the message authentication algorithm supported by the SSH server is SHA1. **sha1-96:** Indicates that the message authentication algorithm supported by the SSH server is SHA1-96.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the message authentication algorithm supported by the SSH server. On Hostname devices, the SSHv1 server does support any message authentication algorithm; the SSHv2 server supports the MD5**,** SHA1**,** SHA1-96**, and** MD5-96 message authentication algorithms. You can select message authentication algorithms supported by the SSH server as required.

Setting A Monitoring Port ID for the SSH Server

Command	**ip ssh port** *port*
Parameter Description	*port*: Indicates the monitoring port ID of the SSH server. The value ranges from 1025 to 65535.
Command Mode	Global configuration mode
Usage Guide	Use either the **no ip ssh port** or the **ip ssh port 22** to restore the monitoring port ID of the SSH server to the default value.

Configuring RSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key rsaflash**:*rsa.pub*

Parameter Description	*test*: Indicates the user name. **rsa:** Indicates that the public key type is RSA. *rsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the RSA public key file associated with user *test*. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Configuring DSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key dsaflash**:*dsa.pub*
Parameter Description	*test*: Indicates the user name. **dsa**: Indicates that the public key type is DSA. *dsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the DSA key file associated with user **test**. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Enabling the SSHv1 Function

Command	**ip ssh compatible-ssh1x enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Minimum Length of the Key Generated by the Key Exchange Algorithm of the SSH Server

Command	**ip ssh dh-exchange min-len { 1024 | 2048 }**
Parameter Description	**1024**: Sets the minimum length of the key generated by the key exchange algorithm of the SSH server to 1024 bytes. **2048**: Sets the minimum length of the key generated by the key exchange algorithm of the SSH server to 2048 bytes.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling the IP Address Blocking Function on the SSH Server

Command	**ip ssh ip-block disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When the number of authentication failures for logging to a device through SSH reaches the configured limit of IP address blocking, 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 period of blocked source IP address reaches the unblocking period requirement.

Configuring the Number of Authentication Failures for Blocking IP Addresses and the Time Period for Counting Authentication Failures on the SSH Server

Command	**ip ssh ip-block failed-times** *failed-times* **period** *period-time*
Parameter Description	*failed-times*: Configures the number of authentication failures for blocking IP addresses. The value range is from 1 to 10. *period-time*: Configures the time period for counting authentication failures in minutes. The value range is from 1 to 120.
Command Mode	Global configuration mode
Usage Guide	After the IP address blocking function is enabled, if the number of consecutive authentication failures for device login through SSH reaches the configured limit in an authentication failure count period, the source IP address is blocked. If the number of consecutive authentication failures does not reach the configured limit in an authentication failure count period, or one authentication succeeds, the authentication failures are cleared.

Configuring the Time Period for Unblocking Blocked IP Addresses on the SSH Server

Command	**ip ssh ip-block reactive** *reactive-interval*
Parameter Description	*reactive-interval*: Configures the time period for awakening blocked IP addresses in minutes. The value range is from 1 to 1000.
Command Mode	Global configuration mode
Usage Guide	After the time period for awakening the blocked source IP address reaches the requirement, the entry with the blocked source IP address is cleared. An SSH client can use this IP address to log in to the device.

Configuring the Diffie–Hellman (DH) Algorithm Supported by the SSH Server

Command	**ip ssh key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** | **ecdh_sha2_nistp256** | **ecdh_sha2_nistp384** | **ecdh_sha2_nistp521** }
Parameter Description	**dh_group_exchange_sha1**: Sets the DH algorithm to diffie-hellman-group-exchange-sha1. The default key length is 2048 bytes and unconfigurable. **dh_group14_sha1**: Sets the DH algorithm to diffie-hellman-group14-sha1. The key length is 2048 bytes. **dh_group1_sha1**: Sets the DH algorithm to diffie-hellman-group1-sha1. The key length is 1024 bytes.

	ecdh_sha2_nistp256: Sets the DH algorithm to ecdh_sha2_nistp256. The key length is 256 bytes. **ecdh_sha2_nistp384**: Sets the DH algorithm to ecdh_sha2_nistp384. The key length is 384 bytes. **ecdh_sha2_nistp521**: Sets the DH algorithm to ecdh_sha2_nistp521. The key length is 521 bytes.
Command Mode	Global configuration mode
Usage Guide	By default, SSHv1 servers support no DH algorithm. SSHv2 servers support diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, ecdh_sha2_nistp256, ecdh_sha2_nistp384, and ecdh_sha2_nistp521.

Configuration Example

The following configuration examples describe only configurations related to SSH.

Generating a Public Key on the SSH Server

Configuration Steps	● Run the **crypto key generate { rsa | dsa }** command to generate a RSA public key for the server.
SSH Server	Hostname#configure terminal Hostname(config)# crypto key generate rsa 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. How many bits in the modulus [512]: ● If the generation of the RSA key is successful, the following information is displayed: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] ● If the generation of the RSA key fails, the following information is displayed: % Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]
Verification	● Run the **show crypto key mypubkey rsa** command to display the public information about the RSA key. If the public information about the RSA key exists, the RSA key has been generated.
SSH Server	Hostname(config)#show crypto key mypubkey rsa % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA1 private

	Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU 8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFlKDj1j 0dKBcCfN tr0r/CT+ cs5tlGKV S0ICGifz oB+pYaE= % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEAAQAAAHJfLwKnzOgO F3RIKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISgIfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEYXCFaaxU=

Specifying the SSH Version

Configuration Steps	● Run the **ip ssh version** { **1 | 2** } command to set the version supported by the SSH server to SSHv2.
SSH Server	Hostname#configure terminal Hostname(config)#ip ssh version 2
Verification	● Run the **show ip ssh** command to display the SSH version currently supported by the SSH server.
SSH Server	Hostname(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the SSH Authentication Timeout

Configuration Steps	● Run the **ip ssh time-out** *time* command to set the SSH authentication timeout to 100s.
SSH Server	Hostname#configure terminal

	Hostname(config)#ip sshtime-out100
Verification	● Run the **show ip ssh** command to displaythe configured SSH authentication timeout.
SSH Server	Hostname(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the Maximum Number of SSH Authentication Retries

Configuration Steps	● Run the **ip ssh authentication-retries** *retry times* command to set the maximum number of user authentication retries on the SSH server to 2.
SSH Server	Hostname#configure terminal Hostname(config)#ip ssh authentication-retries 2
Verification	● Run the **show ip ssh** command to displaythe configured maximum number of authentication retries.
SSH Server	Hostname(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Specifying the SSH Encryption Mode

Configuration Steps	● Run the **ip ssh cipher-mode** {**cbc** | **ctr** | **others** }command to set the encryption mode supported by the SSH server to CTR.
SSH Server	Hostname#configure terminal Hostname(config)# ip ssh cipher-mode ctr
Verification	● Select the CTR encryption mode on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.

Specifying the SSH Message Authentication Algorithm

Configuration Steps	● Run the **ip ssh hmac-algorithm** {**md5** | **md5-96** | **sha1** | **sha1-96** } command to set the message authentication algorithm supported bythe SSH server to SHA1.

SSH Server	Hostname#configure terminal Hostname(config)# ip ssh hmac-algorithmsha1
Verification	● Select the SHA1 message authentication algorithm on the SSH client, and verify whether you can successfullylog in to the SSH server from the SSH client.

Setting A Monitoring Port ID for the SSH Server

Configuration Steps	● Run the **ip ssh port** *port* command to set a monitoring port ID to 10000.
SSH Server	Hostname# configure terminal Hostname(config)# ip ssh port 10000
Verification	● Run the show ip ssh command to display information about a monitoring port ID for the SSH server. Hostname(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 10000 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the Public Key Authentication

Configuration Steps	● Run the **ip ssh peer** *username* **public-key** { **rsa** | **dsa**}*filename* command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA) is specified based on the user name.
SSH Server	Hostname#configure terminal Hostname(config)# ip ssh peer test public-keyrsaflash:rsa.pub
Verification	● Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Configuring SSH Device Management

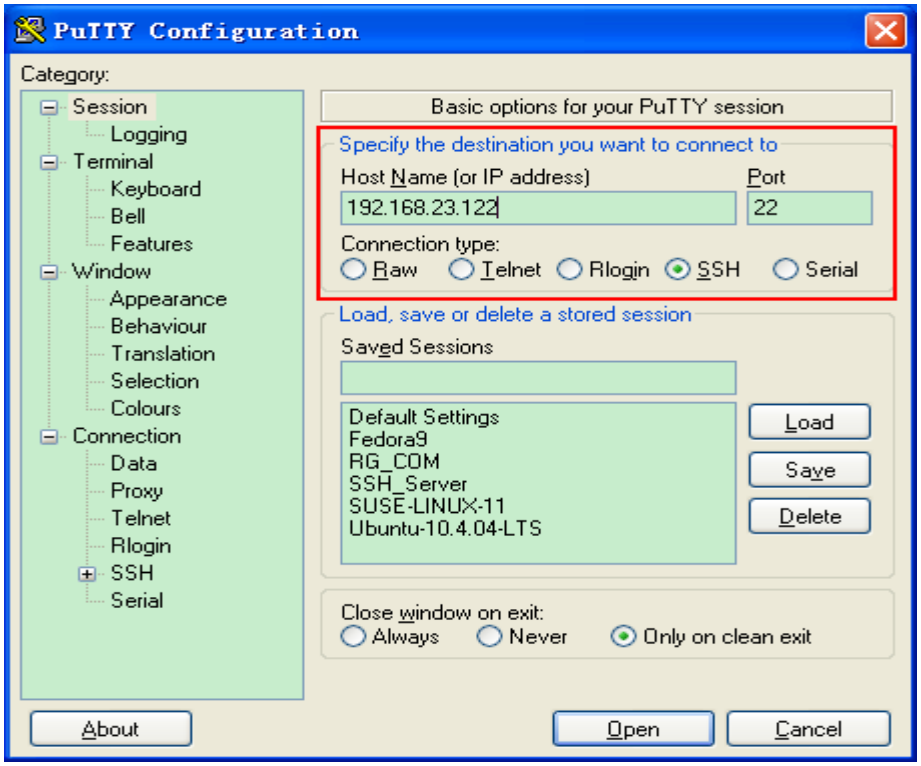
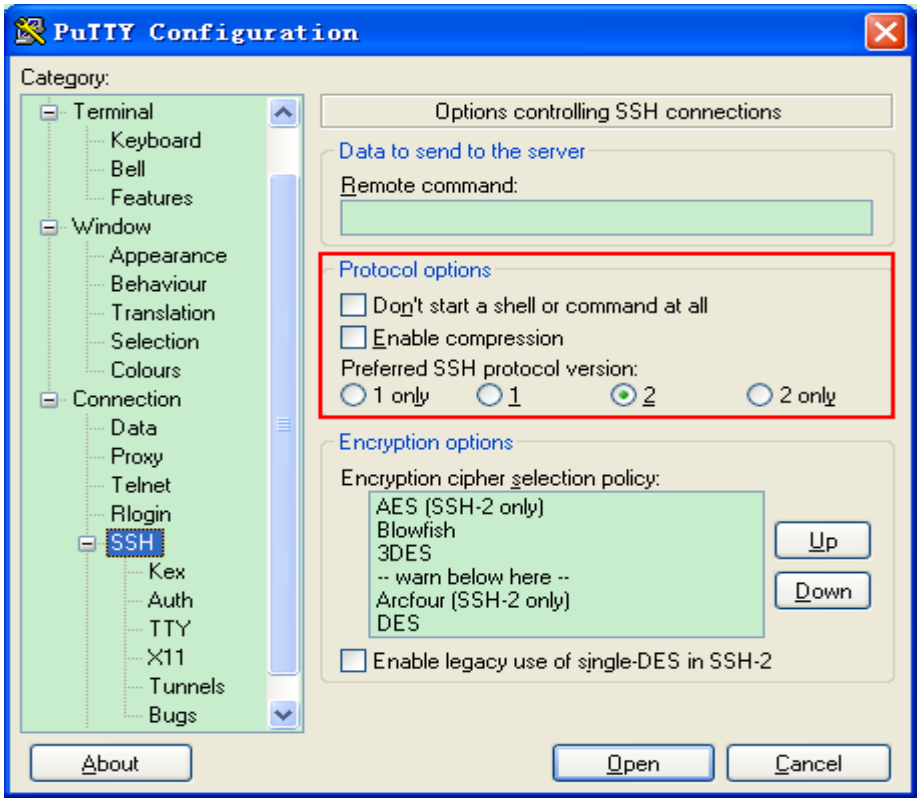
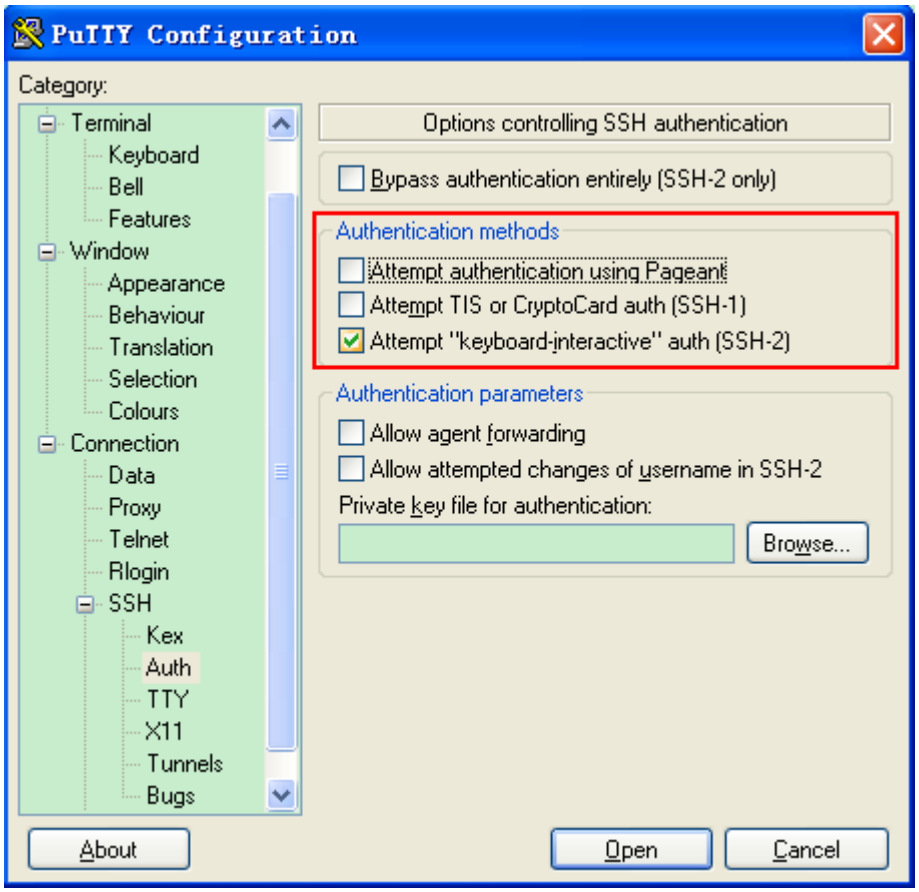
Scenario **Figure 10-6**	 You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible client software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.
Configuration Steps	● Start the PuTTY software. ● On the **Session** option tab of PuTTY, type in the host IP address **192.168.23.122** and SSH port number **22**, and select the connection type **SSH**. ● On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**. ● On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**. ● Click **Open** to connect to the SSH server. ● Type in the correct user name and password to enter the terminal login interface.
SSH Client	Figure 10-7  **Host Name (or IP address)** indicates the IP address of the host to be logged in. In this example, the IP address is **192.168.23.122**. **Port** indicates the port ID 22, that is, the default ID of the port listened by SSH. **Connection type** is **SSH**.

Figure 10-8



As shown in Figure 10-8, select **2** as the preferred SSH protocol version in the **Protocol options** pane because SSHv2 is used for login.

Figure 10-9



As shown in Figure 10-9, select **Attempt "keyboard-interactive" auth** as the authentication method to support authentication based on the user name and password.

Then, click **Open** to connect to the configured server host, as shown in Figure 10-9.

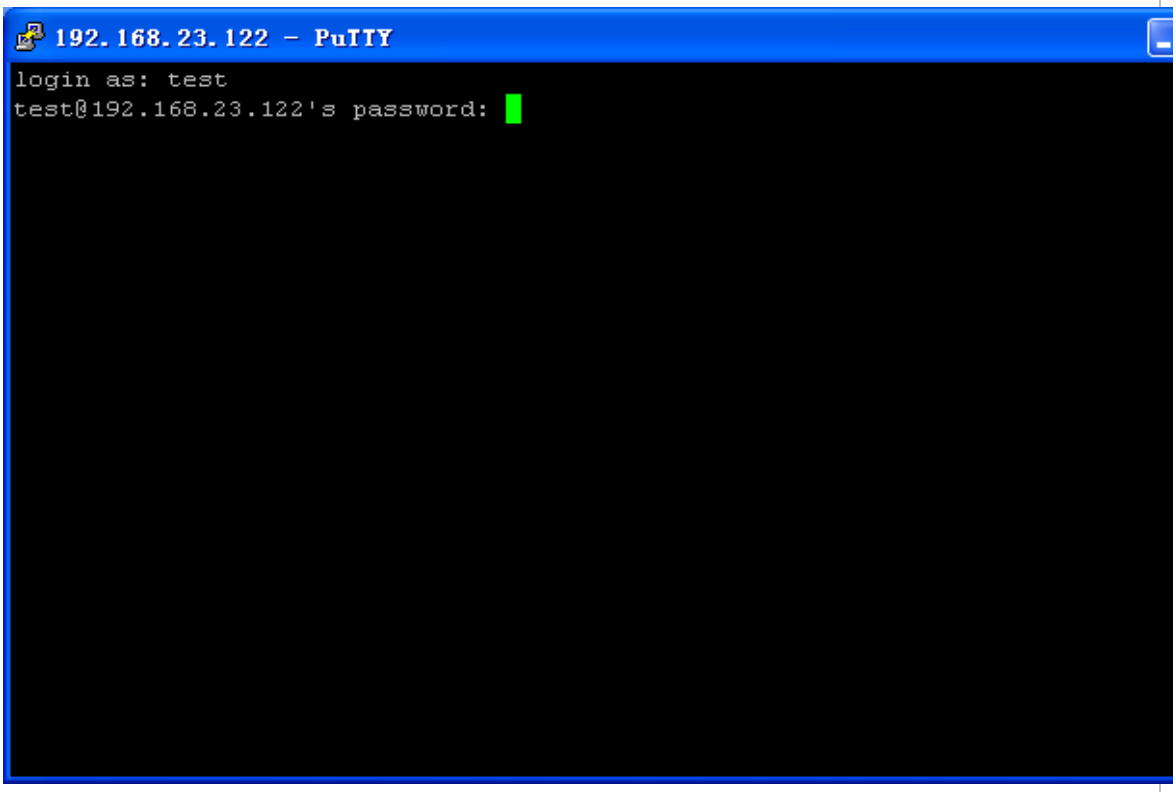
Figure 10-10



The **PuTTY Security Alert** box indicates that you are logging in to the client of the server 192.168.23.122, and asks you whether to receive the key sent from the server.

If you select **Yes**, a login dialog box is displayed, as shown in Figure 10-11.

Figure 10-11

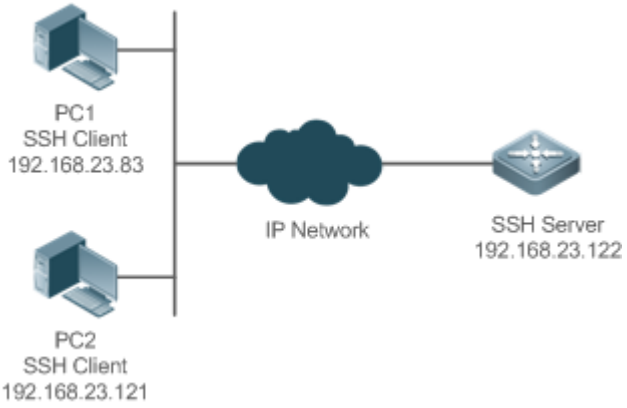


Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 10-12.

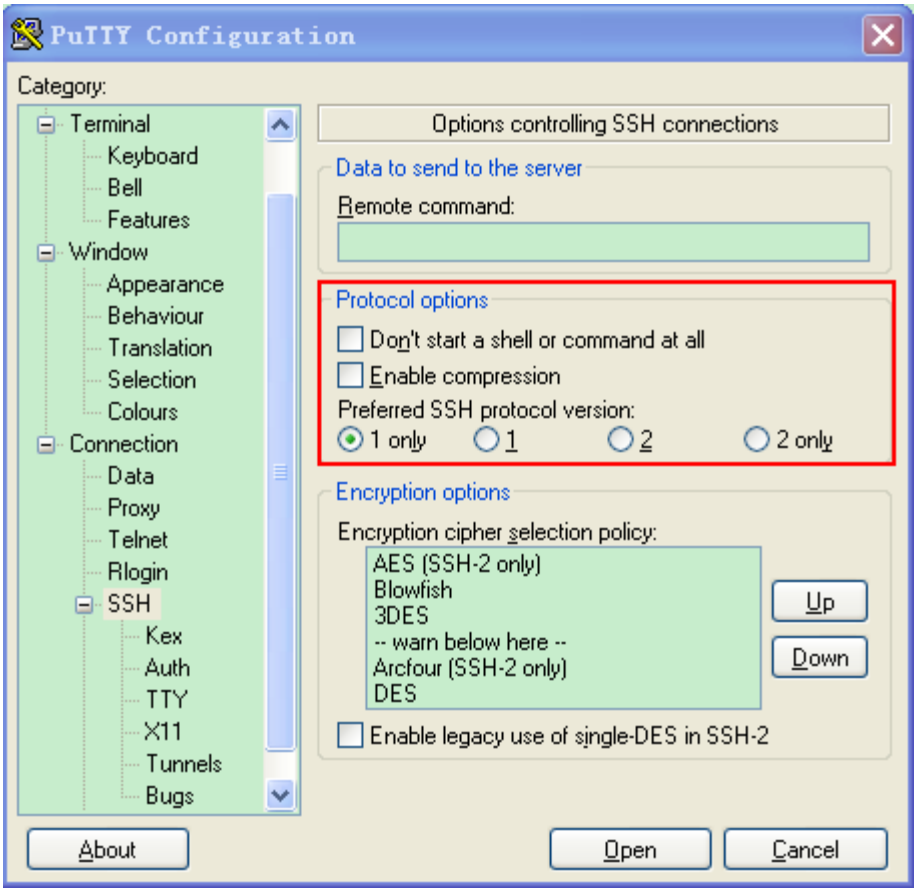
Figure 10-12

	
Verification	● Run the **show ip ssh** command to display the configurations that are currently effective on the SSH server. ● Run the **show ssh** command to display information about every SSH connection that has been established.
	Hostname#show ip ssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 Hostname#show ssh Connection Version Encryption Hmac State Username 0 2.0 aes256-cbc hmac-sha1 Session started test

Configuring SSH Local Line Authentication

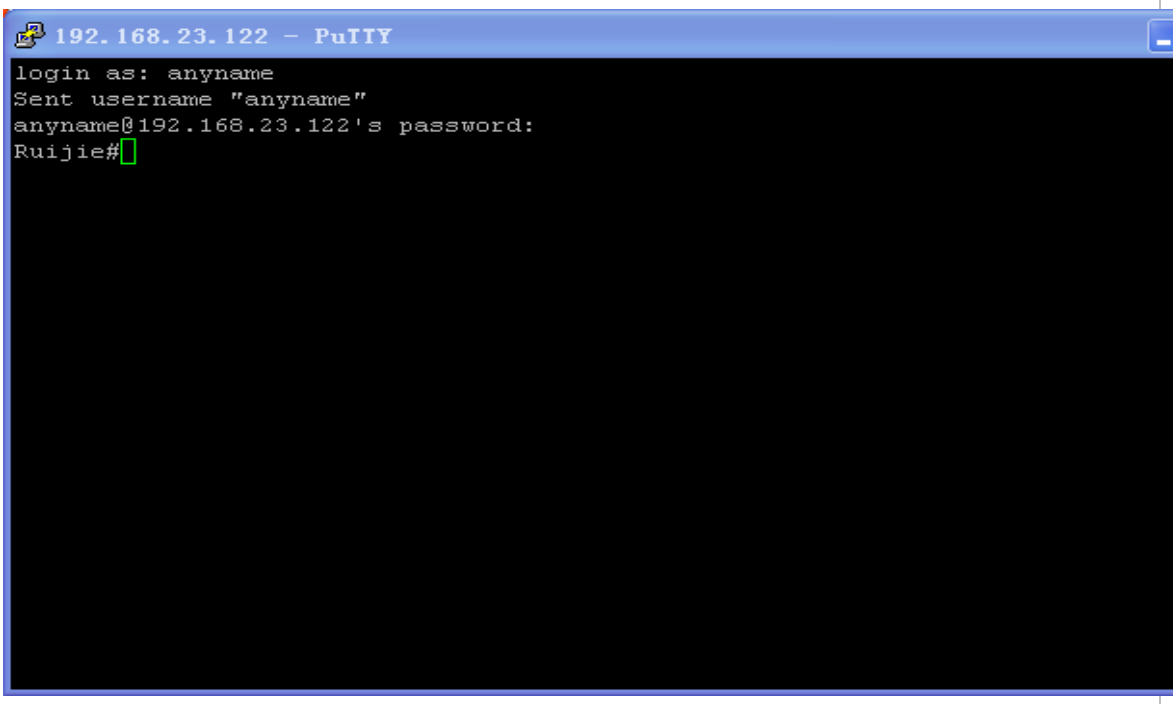
Scenario **Figure 10-13**	 SSH users can use the local line password for user authentication, as shown in Figure 10-13.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server is enabled. The requirements are as follows: ● SSH users use the local line password authentication mode. ● Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.
Configuration Steps	Configure the SSH server as follows: ● Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. ● Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ● Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH client to the SSH server is reachable. Configure the SSH client as follows: ● Diversified SSH client software is available, including PuTTY, Linux, and SecureCRT. This document takes PuTTY as an example to explain the method for configuring the SSH client. For details about the configuration method, see "Configuration Steps."
SSH Server	Before configuring SSH-related function, ensure that the route from the SSH user to the network segment of the SSH server is reachable. The interface IP address configurations are shown in **Figure 10-13**. The detailed procedures for configuring IP addresses and routes are omitted. 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]: Choose the size of the key modulus in the range of 360 to 2048 for your

	Signature Keys. Choosing a key modulus greater than 512 maytake a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Hostname(config)#interface fastEthernet0/1 Hostname(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0 Hostname(config-if-fastEthernet0/1)#exit Hostname(config)#line vty 0 Hostname(config-line)#password passzero Hostname(config-line)#privilege level 15 Hostname(config-line)#login Hostname(config-line)#exit Hostname(config)#line vty1 4 Hostname(config-line)#password pass Hostname(config-line)#privilege level 15 Hostname(config-line)#login Hostname(config-line)#exit
SSH Client(PC1/ PC2)	Figure 10-14



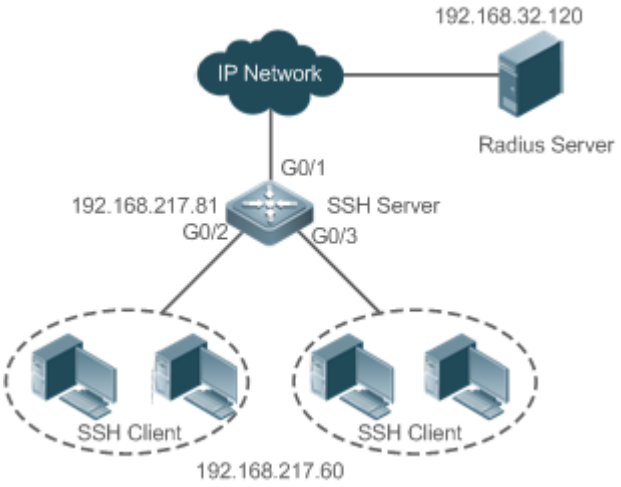
Set the IP address and port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22 (For details about the configuration method, see "Configuring SSH Device Management."). Click **Open** to start the SSH server. As the current authentication mode does not require a user name, you can type in any user name, but cannot leave the user name unspecified. (In this example, the user name is "anyname".)

Verification	● Run the **show running-config** command to display the current configurations. ● Verify that the SSH client configurations are correct.
SSH Server	Hostname#show running-config Building configuration... ! enable secret 5 1eyy2$xs28FDw4s2q0tx97 enable service ssh-server ! interface fastEthernet0/1 ip address 192.168.23.122 255.255.255.0

	! line vty 0 privilege level 15 login password passzero line vty 1 4 privilege level 15 login password pass ! end
SSH Client	Set up a connection, and enter the correct password. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Then, the SSH server operation interface is displayed, as shown in Figure 10-15. Figure 10-15  Hostname#show users Line User Host(s) Idle Location ---------- ---------- ---------- ---------- ---------- * 0 con 0 --- idle 00:00:00 ---

	1 vty 0	---	idle	00:08:02	192.168.23.83
	2 vty 1	---	idle	00:00:58	192.168.23.121

Configuring AAA Authentication of SSH Users

Scenario **Figure 10-16**	 SSH users can use the AAA authentication mode for user authentication, as shown in **Figure 10-16**.To ensure security of data exchange, the PC functions as the SSH client, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, select the local authentication method.
Configuration Steps	● The route from the SSH client to the SSH server is reachable, and the route from the SSH server to the Radius server is also reachable. ● Configure the SSH server on the network device. The configuration method is already described in the previous example, and therefore omitted here. ● Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.
SSH Server	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]: Choose the size of the 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. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Hostname(config)#crypto key generate dsa Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 maytake a few minutes. How many bits in the modulus [512]: % Generating 512 bit DSA keys ...[ok] Hostname(config)#interface gigabitEthernet1/1 Hostname(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0 Hostname(config-if-gigabitEthernet1/1)#exit Hostname#configure terminal Hostname(config)#aaa new-model Hostname(config)#radius-server host 192.168.32.120 Hostname(config)#radius-server key aaaradius Hostname(config)#aaa authentication login methodgroup radius local Hostname(config)#line vty 0 4 Hostname(config-line)#login authentication method Hostname(config-line)#exit Hostname(config)#username user1 privilege 1 password 111 Hostname(config)#username user2 privilege 10 password 222 Hostname(config)#username user3 privilege 15 password 333 Hostname(config)#enable secret w
Verification	● Run the **show running-config** command to displaythe current configurations. ● This example assumes that the SAM server is used. ● Set up a remote SSH connection on the PC. ● Check the login user.
	Hostname#show run aaa new-model

```
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet1/1
 no ip proxy-arp
ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
End
```

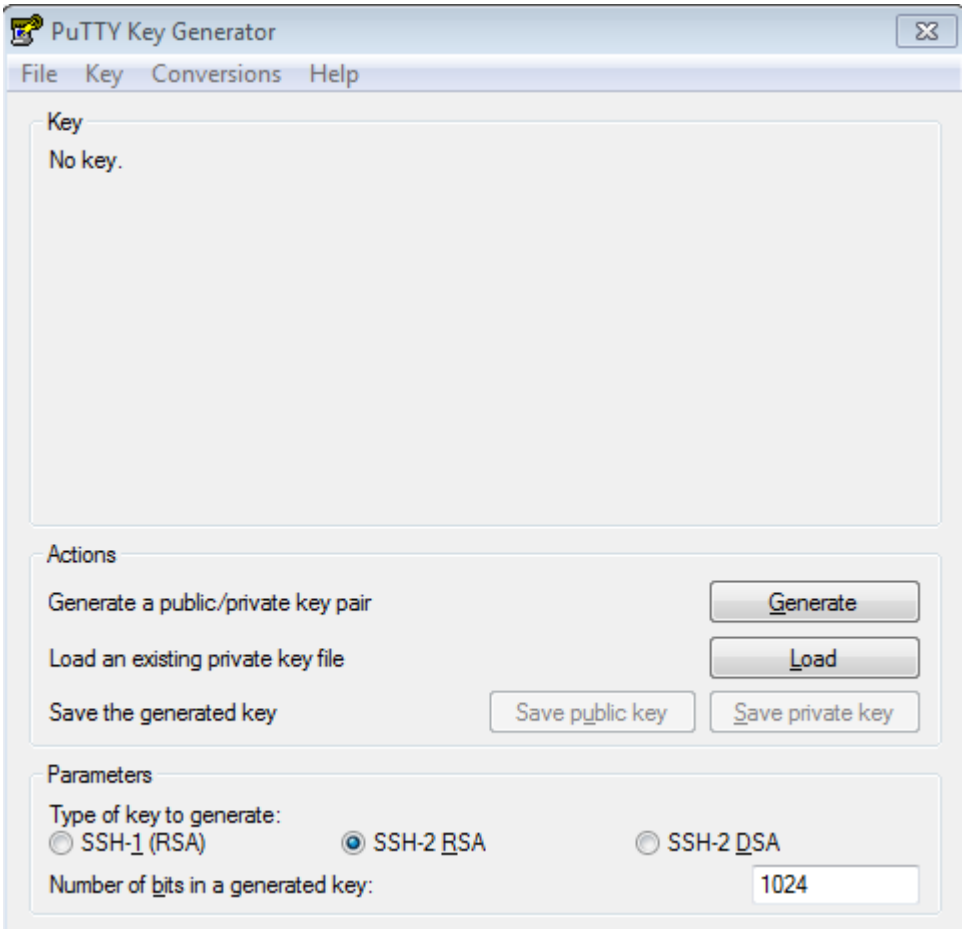
On the SSH client, choose **System Management**>**Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**.
Choose **Security Management**>**Device Management Rights**, and set the rights of the login user.
Choose **Security Management**>**Device Administrator**, and add the user name **user** and password **pass**.
Configure the SSH client and set up a connection to the SSH server. For details, see the previous example.
Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
Hostname#show users
```

	Line User Host(s) Idle Location 0 con 0 idle 00:00:31 * 1 vty 0 user idle 00:00:33 192.168.217.60

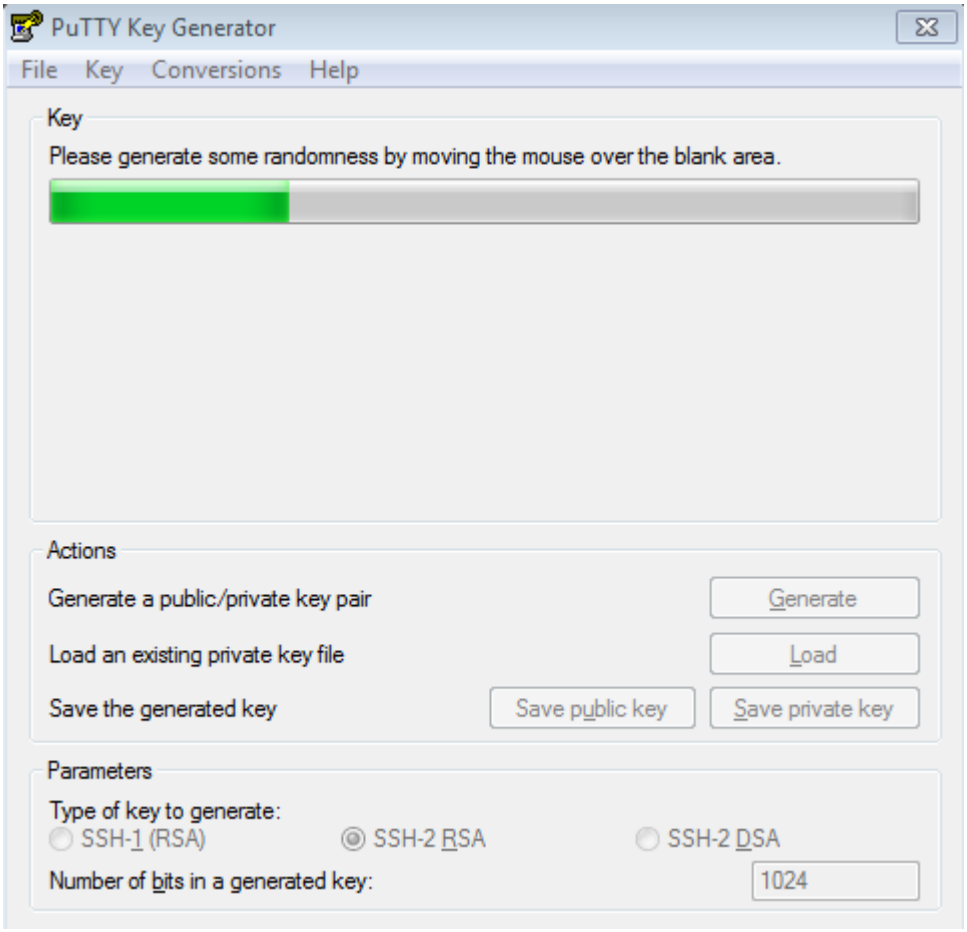
Configuring Public Key Authentication of SSH Users

Scenario **Figure 10-17**	 SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in **Figure 10-17**.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.
Configuration Steps	● To implement public key authentication on the client, generate a key pair (for example, RSA key) on the client, place the public key on the SSH server, and select the public key authentication mode. After the key pair is generated on the client, you must save and upload the public key file to the server and complete the server-related settings before you can continue to configure the client and connect the client with the server. ● After the key is generated on the client, copy the public key file from the client to the flash of the SSH server, and associate the file with an SSH user name. A user can be associated with one RSA public key and one DSA public key.
SSH Client	Run the **puttygen.exe** software on the client. Select **SSH-2 RSA** in the **Parameters** pane, and click **Generate** to generate a key, as shown in Figure 10-18. Figure 10-18



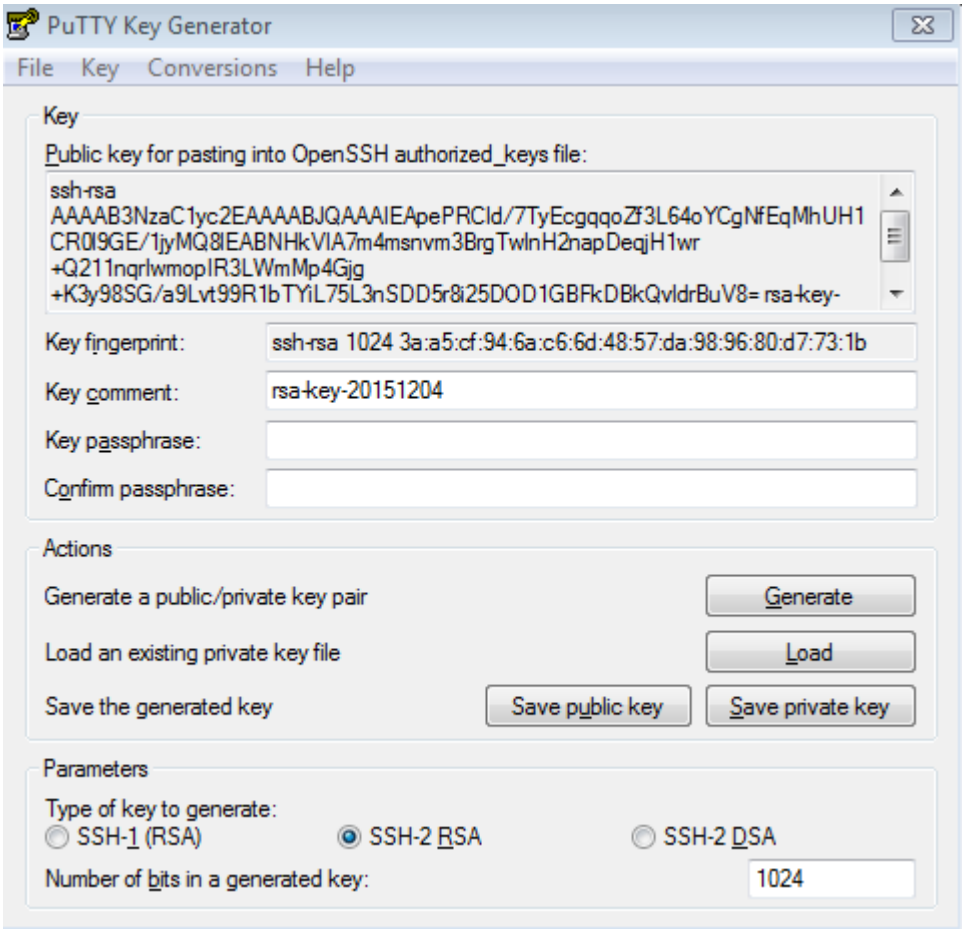
When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 10-19.

Figure 10-19



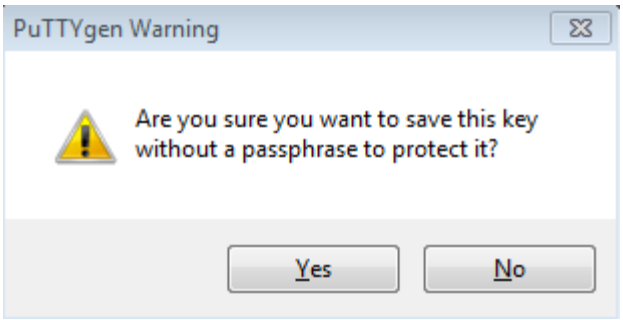
To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1,024 bits.

Figure 10-20



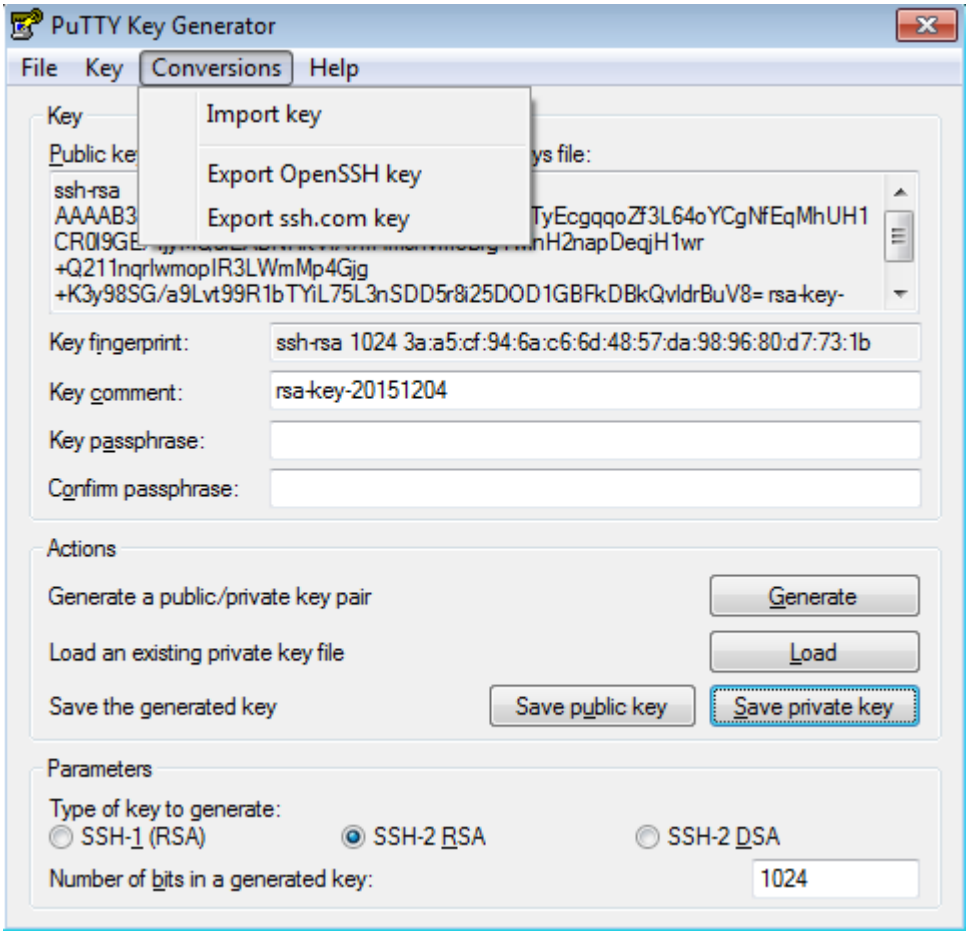
After the key pair is generated, click **Save public key**, type in the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following prompt box is displayed. Select **Yes**, type in the public key name **test_private**, and click **Save**.

Figure 10-21

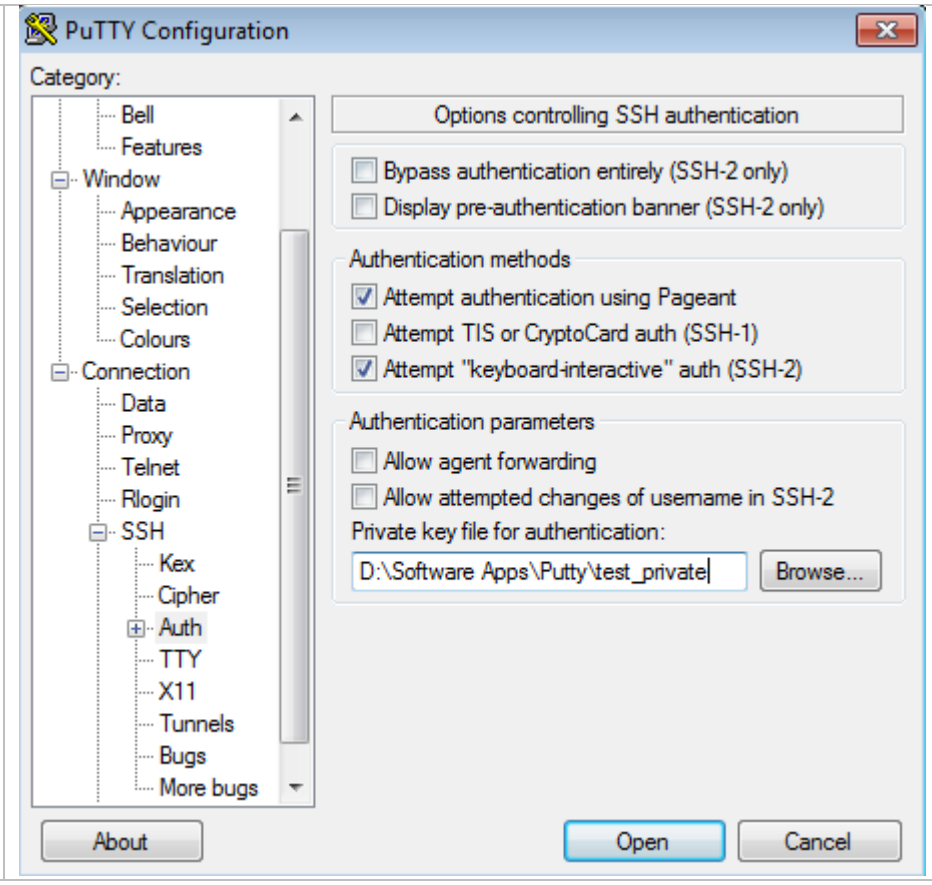


You must select the OpenSSH key file; otherwise, the key file cannot be used. The **puttygen.exe** software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. Format conversion is not required for the public key file stored on the server, and the format of this file is still OpenSSH, as shown in Figure 10-22.

Figure 10-22



SSH Server	Hostname#configure terminal Hostname(config)# ip ssh peer test public-key rsa aflash:test_key.pub
Verification	● After completing the basic configurations of the client and the server, specify the private key file **test_private** on the PuTTY client, and set the host IP address to **192.168.23.122** and port ID to **22** to set up a connection between the client and the server. In this way, the client can use the public key authentication mode to log in to the network device.
	Figure 10-23



Common Errors

- The **no crypto key generate** command is used to delete a key.

10.4.2 Configuring the SCP Service

Configuration Effect

After the SCP function is enabled on a network device, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

Notes

- The SSH server must be enabled in advance.

Configuration Steps

Enabling the SCP Server

- Mandatory.
- By default, the SCP server function is disabled. Run the **ip scp server enable** command to enable the SCP server function in global configuration mode.

Verification

Run the **show ip ssh** command to check whether the SCP server function is enabled.

Related Commands

Enabling the SCP Server

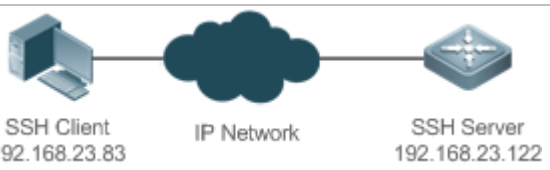
Command	**ip scp server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to enable the SCP server. Run the **no ip scp server enable** command to disable the SCP server.

Configuration Example

Enabling the SCP Server

Configuration Steps	● Run the **ip scp server enable** command to enable the SCP server.
	Hostname#configure terminal Hostname(config)#ip scp server enable
Verification	● Run the **show ip ssh** command to check whether the SCP server function is enabled.
	Hostname(config)#show ipssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled

Configuring SSH File Transfer

Scenario Figure 10-24	 The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.
Configuration	● Enable the SCP service on the server.

Steps	The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can finds out that the user type is SSH by running the show user command). ● On the client, use SCP commands to upload files to the server, or download files from the server. Syntax of the SCP command: scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 [...] [[user@]host2:]file2 Descriptions of some options: -1: Uses SSHv1 (If not specified, SSHv2 is used by default); -2: Uses SSHv2 (by default); -C: Uses compressed transmission. -c: Specifies the encryption algorithm to be used. -r:Transmits the whole directory; -i: Specifies the key file to be used. -l: Limits the transmission speed (unit: Kbit/s). For other parameters, see the filescp.0. Most options are related to terminals. Few options are supported on both terminals and servers. Hostname's SCP servers do not support d-p-q-r options. When these options are applied, there are prompts.
SSH Server	Hostname#configure terminal Hostname(config)# ip scp server enable
Verification	● File transmission example on the Ubuntu 7.10 system: Set the username of a client to **test** and copy the **config.text** file from the network device with the IP address of 192.168.195.188 to the **/root** directory on the local device.
	root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text 100% 1506 1.5KB/s 00:00 Read from remote host 192.168.195.188: Connection reset by peer

10.4.3 Configuring the SSH Client

Configuration Effect

On the network device that supports the SSH server, enable the SSH server function, and specify the user authentication method and supported SSH versions. Then, you can use the built-in SSH client function of the device to set up a secure connection with the SSH server, implementing remote device management.

Notes

- The SSH server function must be configured in advance on the device that needs to remotely support the SSH server.
- The SSH client must communicate with the SSH server properly.

Configuration Steps

Specifying the Source Interface of the SSH Client

- (Optional) This configuration must be performed on the SSH-client device.

Establishing a Session with the SSH Server

- (Optional) Use the **ssh** command on the client to set up a connection with a remote server.
- Before using this command, enable the SSH server function and configure the SSH key and authentication mode on the server.

Recovering an Established SSH Session

- (Optional) Run the related command to recover a session after temporary stop if necessary.

Disconnecting a Suspended SSH Session

- (Optional) This configuration must be performed on the SSH client if you need to disconnect a specified SSH session.

Verification

Run the **show ssh-session** command to display information about every established SSH client session.

Related Commands

Specifying the Source Interface of the SSH Client

Command	**ip ssh source-interface** *interface-name*
Parameter Description	*interface-name*: Specifies an interface, the IP address of which will be used as the source address of an SSH client session.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify an interface, the IP address of which will be used as the global source address of an SSH client session. When the **ssh** command is used to connect to an SSH server, this global configuration will be used if a source interface or a source address is not specified for this connection. Run the **no ip ssh source-interface** command to restore the default setting.

Establishing a Session with the SSH Server

Command	**ssh** [**oob**] [**-v** {**1** | **2** }][**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*] [**-m** {**hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }] [**-p** *port-num*] { *ip-addr*| *hostname*} [**/source** {**ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name*}] [**/vrf** *vrf-name*]
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	The **ssh** command is used to set up a secure and encrypted connection from the local device (an SSH client) to another device (an SSH server) or any other server that supports SSHv1 or SSHv2. This connection provides a mechanism similar to the Telnet connection except that all data transmitted over this connection is encrypted. Based on authentication and encryption, the SSH client can set up a secure connection on an insecure network. ⚠ 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, and AES256-CBC. ⚠ SSHv1 does not support the Hashed Message Authentication Code (HMAC). ⚠ If you specify an unmatched encryption or authentication algorithm when selecting an SSH version, the unmatched algorithm will be ignored when a connection is set up.

Recovering an Established SSH Client Session

Command	**ssh-session** *session-id*
Parameter Description	*session-id*: Indicates the ID of an established SSH client session.
Command Mode	User EXEC mode
Usage Guide	This command is used to restore the use of an established SSH client session. When the **ssh** command is used to initiate an SSH client session, you can press Ctrl+Shift+6+X to temporarily exit the session. To recover this session, run the **ssh-session** command. In addition, if the session is already established, you can run the **show ssh-session** command to display information about the established session.

Disconnecting a Suspended SSH Session

Command	**disconnect ssh-session** *session-id*
Parameter Description	*session-id*: Indicates the ID of a suspended SSH client session.
Command Mode	User EXEC mode
Usage Guide	You can specify an SSH client session ID to disconnect the specified SSH client session.

Configuration Example

Specifying the Source Interface of the SSH Client

Configuration Steps	● Run the **ip ssh source-interface** *interface-name* command to specify an interface, the IP address of which will be used as the global source address of an SSH client session.
	Hostname#configure terminal Hostname(config)#ipsshsource-interface gigabitEthernet 0/1
Verification	N/A

Establishing a Session with the SSH Server

Scenario Figure 10-25	 The SSH server function is enabled on the server. The **ssh** command is used on the client to set up a secure connection with the server.
Configuration Steps	● Enable the SSH server function on the server. ● Configure the SSH key on the server. ● Configure the authentication mode of the SSH server, and use the local line authentication mode for Line 0 to Line 4. ● Configure the IP address of the Gi 0/1 interface of the SSH server. The client will use this address as the source address to connect to the SSH server. ● Configure the SSH client, and specify the source address of the SSH client. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. The authentication mode used by the SSH server is local line authentication. The local user name is admin, and the password is 123456. The SSH client is connected to the SSH server based on this IP address. The routes from the SSH clients to the SSH server are reachable. Configure the IP address of the Gi 0/1 interface of the SSH server. The client will use this address as the source address to connect to the SSH server.
SSH Server	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]: Choose the size of the 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. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Hostname(config)#line vty 0 4 Hostname(config-line)#login local Hostname(config-line)#exit Hostname(config)#username admin password 123456 Hostname(config)#username admin privilege 15 Hostname(config-line)#exit Hostname(config)#interface gigabitEthernet0/1 Hostname(config-if-gigabitEthernet0/1)#ip address 192.168.23.122 255.255.255.0 Hostname(config-if-gigabitEthernet0/1)#exit
SSH Client	Hostname(config)#interface gigabitEthernet0/1 Hostname(config-if-gigabitEthernet0/1)#ip address 192.168.23.83 255.255.255.0 Hostname(config-if-gigabitEthernet0/1)#exit Hostname(config)#ipsshsource-interface gigabitEthernet 0/1
Verification	● Run the **show running-config| include username** and **show ip ssh** commands to verify whether the SSH server configurations are correct. ● On the SSH client, set up a connection with a remote SSH server. After the connection is set up, type in the correct password **123456**. The SSH server operation interface is displayed. Check the login user on the Console of the SSH client.
	Hostname(config)#sh running-config | include username username admin password admin username admin privilege 15 Hostname(config)#sh running-config | begin line

	line con 0 line vty 0 4 login local ! ! end
	● Verify whether the SSH client configurations are correct.
	Hostname#ssh -l admin 192.168.23.122 %Trying 192.168.23.122, 22,...open admin@192.168.23.122's password: Hostname# Hostname#sh users Line User Host(s) Idle Location 0 con 0 idle 00:00:00 * 1 vty 0 admin idle 00:00:36 192.168.217.20

10.5 Monitoring

Displaying

Description	Command
Displays the effective SSH server configurations.	**show ipssh**
Displays the established SSH connection.	**show ssh**
Displays the public information of the SSH public key.	**show crypto key mypubkey**
Displays the established SSH client session.	**show ssh-session**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs SSH sessions.	**debug ssh**
Debugs SSH client sessions.	**debug ssh client**

11 Configuring CPP

11.1 Overview

The CPU Protect Policy (CPP) provides policies for protecting the CPU of a switch.

In network environments, various attack packets spread, which may cause high CPU usages of the switches, affect protocol running and even difficulty in switch management. To this end, switch CPUs must be protected, that is, traffic control and priority-based processing must be performed for various incoming packets to ensure the processing capabilities of the switch CPUs.

CPP can effectively prevent malicious attacks in the network and provide a clean environment for legitimate protocol packets.

CPP is enabled by default. It provides protection during the entire operation of switches.

11.2 Applications

Application	Description
Preventing Malicious Attacks	When various malicious attacks such as ARP attacks intrude in a network, CPP divides attack packets into queues of different priorities so that the attack packets will not affect other packets.
Preventing CPU Processing Bottlenecks	Even when no attacks exist, it would become a bottleneck for CPU to handle excessive normal traffic. CPP can limit the rate of packets being sent to the CPU to ensure normal operation of switches.

11.2.1 Preventing Malicious Attacks

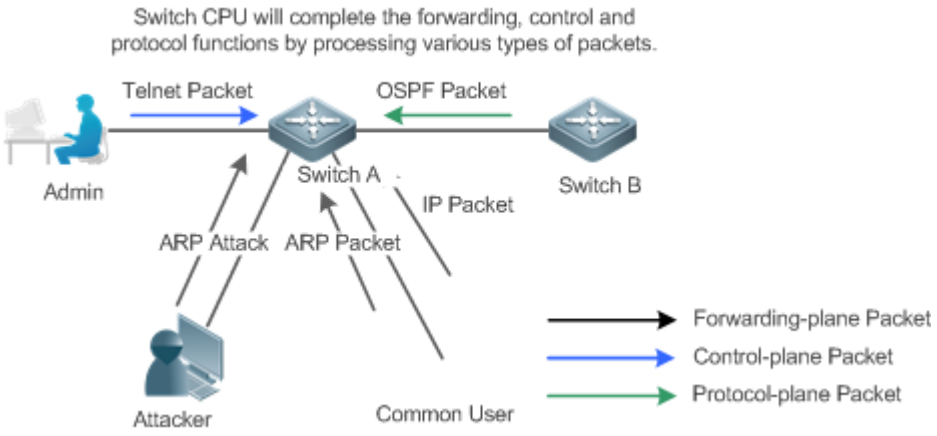
Scenario

Network switches at all levels may be attacked by malicious packets, typically ARP attacks.

As shown in Figure 11-1, switch CPUs process three types of packets: forwarding-plane, control-plane and protocol-plane. Forwarding-plane packets are used for routing, including ARP packets and IP route disconnection packets. Control-plane packets are used to manage services on switches, including Telnet packets and HTTP packets. Protocol-plane packets serve for running protocols, including BPDU packets and OSPF packets.

When an attacker initiates attacks by using ARP packets, the ARP packets will be sent to the CPU for processing. Since the CPU has limited processing capabilities, the ARP packets may force out other packets (which may be discarded) and consume many CPU resources (for processing ARP attack packets). Consequently, the CPU fails to work normally. In the scenario as shown in Figure 11-1, possible consequences include: common users fail to access the network; administrators fail to manage switches; the OSPF link between switch A and the neighbor B is disconnected and route learning fails.

Figure 11-1 Networking Topology of Switch Services and Attacks



Deployment

- By default, CPP classifies ARP packets, Telnet packets, IP route disconnection packets, and OSFP packets into queues of different priorities. In this way, ARP packets will not affect other packets.
- By default, CPP limits the rates of ARP packets and the rates of the priority queue where the ARP packets reside to ensure that the attack packets do not occupy too many CPU resources.
- Packets in the same priority queue with ARP packets may be affected by ARP attack packets. You can divide the packets and the ARP packets into different priority queues by means of configuration.
- When ARP attack packets exist, CPP cannot prevent normal ARP packets from being affected. CPP can only differentiate the packet type but cannot distinguish attack packets from normal packets of the same type. In this case, the Network Foundation Protection Policy (NFPP) function can be used to provide higher-granularity attack prevention.

For description of NFPP configurations, see the *Configuring NFPP*.

11.2.2 Preventing CPU Processing Bottlenecks

Scenario

Even though no attacks exist, many packets may need to be sent to the CPU for processing at an instant.

For example, the accesses to the core device of a campus network are counted in ten thousands. The traffic of normal ARP packets may reach dozens of thousands packets per second (PPS). If all packets are sent to the CPU for processing, the CPU resources cannot support the processing, which may cause protocol flapping and abnormal CPU running.

Deployment

- By default, the CPP function limits the rates of ARP packets and the rates of the priority queue where the APR packets reside to control the rate of ARP packets sent to the CPU and ensure that the CPU resource consumption is within a specified range and that the CPU can normally process other protocols.
- By default, the CPP function also limits the rates of other packets at the user level, such as Web authentication and 802.1X authentication packets.

11.3 Features

Basic Concepts

QOS, DiffServ

Quality of Service (QoS) is a network security mechanism, a technology used to solve the problems of network delay and congestion.

DiffServ refers to the differentiated service model, which is a typical model implemented by QoS for classifying service streams to provide differentiated services.

Bandwidth, Rate

Bandwidth refers to the maximum allowable data rate, which refers to the rate threshold in this document. Packets whose rates exceed the threshold will be discarded.

The rate indicates an actual data rate. When the rate of packets exceeds the bandwidth, packets out of the limit will be discarded. The rate must be equal to or smaller than the bandwidth.

The bandwidth and rate units in this document are packets per second (pps).

L2, L3, L4

The structure of packets is hierarchical based on the TCP/IP model.

L2 refers to layer-2 headers, namely, the Ethernet encapsulation part; L3 refers to layer-3 headers, namely, the IP encapsulation part; L4 refers to layer-4 headers, usually, the TCP/UDP encapsulation part.

Priority Queue, SP

Packets are cached inside a switch and packets in the output direction are cached in queues. Priority queues are mapped to Strict Priorities (SPs). Queues are not equal but have different priorities.

The SP is a kind of QoS scheduling algorithm. When a higher priority queue has packets, the packets in this queue are scheduled first. Scheduling refers to selecting packets from queues for output and refers to selecting and sending the packets to the CPU in this document.

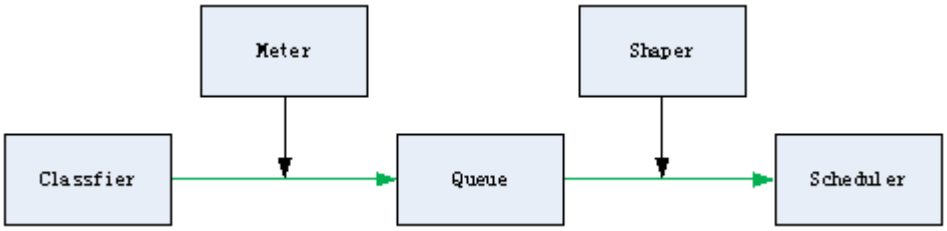
CPU interface

Before sending packets to the CPU, a switch will cache the packets. The process of sending packets to the CPU is similar to the process of packet output. The CPU interface is a virtual interface. When packets are sent to the CPU, the packets will be output from this virtual interface. The priority queue and SP mentioned above are based on the CPU interface.

Overview

CPP protects the CPU by using the standard QoS DiffServ model.

Figure 11-2 CPP Implementation Model



Feature	Description
Classfier	Classifies packet types and provides assurance for the subsequent implementation of QoS policies.
Meter	Limits rates based on packet types and controls the bandwidth for a specific packet type.
Queue	Queue packets to be sent to the CPU and select different queues based on packet types.
Scheduler	Selects and schedules queues to be sent to the CPU.
Shaper	Performs rate limit and bandwidth control on priority queues and the CPU interface.

11.3.1 Classifier

Working Principle

The Classifier classifies all packets to be sent to the CPU based on the L2, L3 and L4 information of the packets. Classifying packets is the basis for implementing QoS policies. In subsequent actions, different policies are implemented based on the classification to provide differentiated services. A switch provides fixed classification. The management function classifies packet types based on the protocols supported by the switch, for example, STP BPDU packets and ICMP packets. Packet types cannot be customized.

11.3.2 Meter

Working Principle

The Meter limits the rates of different packets based on the preset rate thresholds. You can set different rate thresholds for different packet types. When the rate of a packet type exceeds the corresponding threshold, the packets out of the limit will be discarded.

By using the Meter, you can control the rate of a packet type sent to the CPU within a threshold to prevent specific attack packets from exerting large impacts on the CPU resources. This is the level-1 protection of the CPP.

Related Configuration

- By default, each packet type corresponds to a rate threshold (bandwidth) and Meter policies are implemented based on the rate threshold.
- In application, you can run the **cpu-protect type** *packet-type* **bandwidth** *bandwidth-value* command to set Meter policies for specified packet types.

11.3.3 Queue

Working Principle

Queues are used to classify packets at level 2. You can select the same queue for different packet types; meanwhile, queues cache packets inside switches 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.

Related Configuration

- By default, each packet type is mapped to an SP queue.
- In application, you can run the **cpu-protect type** *packet-type* **traffic-class** *traffic-class-num* command to select SP queues for specific packet types.

11.3.4 Scheduler

Working Principle

The Scheduler schedules packets based on SPs of queues. That is, packets in a queue with a higher priority are scheduled first.

Before being scheduled, packets to be sent to the CPU are cached in queues. When being scheduled, the packets are sent to the CPU for processing.

Only the SP scheduling policy is supported and cannot be modified.

11.3.5 Shaper

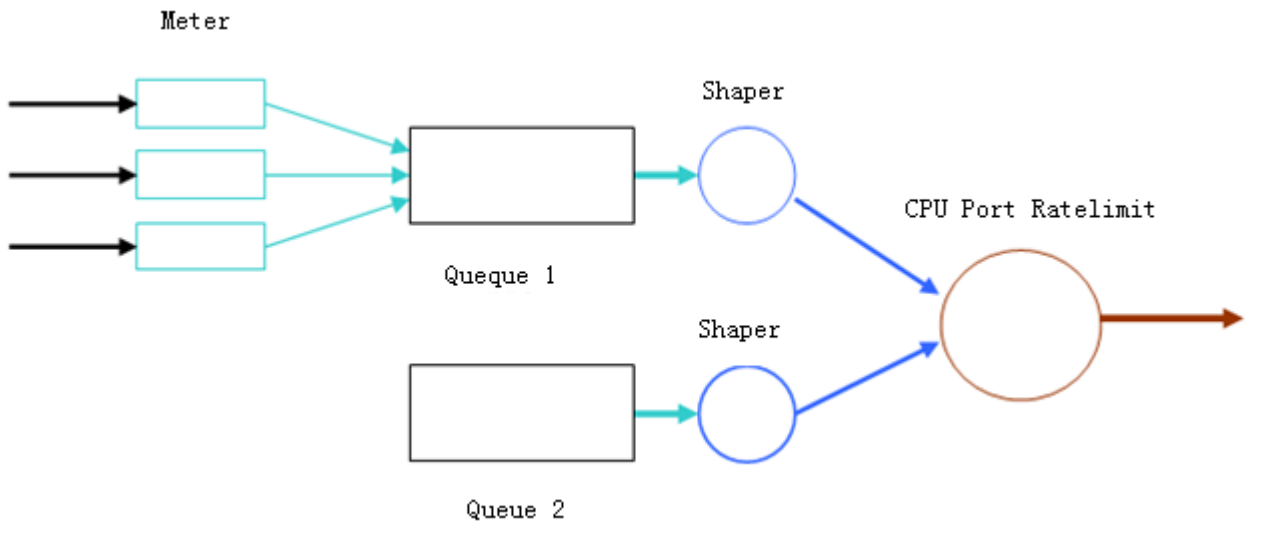
Working Principle

The Shaper is used to shape packets to be sent to the CPU, that is, when the actual rate of packets is greater than the shaping threshold, the packets must stay 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 (no more than the shaping threshold).

When the Shaper is available, packets in a queue with a lower priority may be scheduled before all packets in a queue with a higher priority are scheduled. If the rate of packets in a queue with certain priority exceeds the shaping threshold, scheduling of the packets in this queue may be stopped temporarily. Therefore, the Shaper can prevent packets in queues with lower priorities from starvation (which means that only packets in queues with higher priorities are scheduled and packets in queues with higher priorities are not scheduled).

Since the Shaper limits the scheduling rates of packets, it actually plays the rate limit function. The Shaper provides level-2 rate limit for priority queues and all packets sent to the CPU (CPU interface). The Shaper and Meter functions provide 3-level rate limit together and provide level-3 protection for the CPU.

Figure 11-3 Level Rate Limit of the CPP



Related Configuration

Configuring the Shaper for priority queues

- By default, each priority queue determines a shaping threshold (bandwidth).
- In application, you can run the **cpu-protect traffic-class** *traffic-class-num* **bandwidth** *bandwidth_value* command to perform Shaper configuration for a specific priority queue.

Configuring the Shaper for the CPU Interface

- By default, the CPU interface determines a shaping threshold (bandwidth).
- Run the **cpu-protect cpu bandwidth** *bandwidth_value* command to perform Shaper configuration for the CPU interface.

11.4 Configuration

Configuration	Description and Command	
Configuring CPP	(Optional and configured by default) It is used to adjust the configuration parameters of CPP.	
	cpu-protect type *packet-type* **bandwidth**	Configures the Meter for a packet type.
	cpu-protect type *packet-type* **traffic-class**	Configures the priority queue for a packet type.
	cpu-protect traffic-class *traffic-class-num* **bandwidth**	Configures the Shaper for a priority queue.
	cpu-protect cpu bandwidth	Configures the Shaper for the CPU interface.

11.4.1 Configuring CPP

Configuration Effect

- By configuring the Meter function, you can set the bandwidth and rate limit for a packet type. Packets out of the limit will be directly discarded.
- By configuring the Queue function, you can select a priority queue for a packet type. Packets in a queue with a higher priority will be scheduled first.
- By configuring the Shaper function, you can set the bandwidth and rate limit for a CPU interface and a priority queue. Packets out of the limit will be directly discarded.

Notes

- Pay special attention when the bandwidth of a packet type is set to a smaller value, which may affect the normal traffic of the same type. To provide per-user CPP, combine the NFPP function.
- When the Meter and Shaper functions are combined, 3-level protection will be provided. Any level protection fights alone may bring negative effects. For example, if you want to increase the Meter of a packet type, you also need to adjust the Shaper of the corresponding priority queue. Otherwise, the packets of this type may affect other types of packets in the same priority queue.

Configuration Steps

↘ Configuring the Meter for a packet type

- You can use or modify the default value but cannot disable it.
- You need to modify the configuration in the following cases: when packets of a type are not attackers but are discarded, you need to increase the Meter of this packet type. If attacks of a packet type cause abnormal CPU running, you need to decrease the Meter of this packet type.
- This configuration is available on all switches in a network environment.

↘ Configuring the priority queue for a packet type

- You can use or modify the default value but cannot disable it.
- You need to modify the configuration in the following cases: When attacks of a packet type cause abnormality of other packets in the same queue, you can put the packet type in an unused queue. If a packet type cannot be discarded but the packet type is in the same queue with other packet types in use, you can put this packet type in a queue with a higher priority.
- This configuration is available on all switches in a network environment.

↘ Configuring the Shaper for a priority queue

- You can use or modify the default value and cannot disable it.
- You need to modify the configuration in the following cases: If the Meter value of a packet type is greater which causes that other packets in the corresponding priority queue do not have sufficient bandwidth, you need to increase the

Shaper for this priority queue. If attack packets are put in a priority queue and no other packets are in use, you need to increase the Shaper of this priority queue.

- This configuration is available on all switches in a network environment.

Configuring the Shaper for the CPU interface

- You can use or modify the default value and cannot disable it.
- You are not advised to change the Shaper of the CPU interface.
- This configuration is available on all switches in a network environment.

Verification

- Modify the configurations when the system runs abnormally, and view the system running after the modification to check whether the configurations take effect.
- Check whether the configurations take effect by viewing corresponding configurations and statistic values. For details, see the following commands.

Related Commands

Configuring the Meter for a packet type

Command	**cpu-protect type** *packet-type* **bandwidth** *bandwidth_value*
Parameter Description	*packet-type*: Specifies a packet type. Packet types are defined. *bandwidth_value*: Sets the bandwidth, in the unit of packets per second (pps).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the priority queue for a packet type

Command	**cpu-protect type** *packet-type* **traffic-class** *traffic-class-num*
Parameter Description	*packet-type*: Specifies a packet type. Packet types are defined. *traffic-class-num*: Specifies a priority queue.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Shaper for a priority queue

Command	**cpu-protect traffic-class** *traffic-class-num* **bandwidth** *bandwidth_value*
Parameter Description	*traffic-class-num*: Specifies a priority queue. *bandwidth_value*: Sets the bandwidth, in the unit of pps.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Shaper for a CPU interface

Command	**cpu-protect cpu bandwidth** *bandwidth_value*
Parameter Description	*bandwidth_value*: Sets the bandwidth, in the unit of pps.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Preventing packet attacks and network flapping by using CPP

Scenario	● ARP, IP, OSPF, dot1x, VRRP, Telnet and ICMP streams are available in the system. In the current configurations, ARP and 802.1X are in priority queue 2; IP, ICMP and Telnet streams are in priority queue 4; OSPF streams are in priority queue 3; VRRP streams are in priority queue 6. The Meter for each packet type is 10,000 pps; the shaper for each priority queue is 20,000 pps; the Shaper for the CPU interface is 100,000 pps. ● ARP attacks and IP scanning attacks exist in the system, which causes abnormal running of the system, authentication failure, Ping failure, management failure, and OSPF flapping.
Configuration Steps	● Put ARP attack packets in priority queue 1 and limit the bandwidth for ARP packets or the corresponding priority queue. ● Put OSPF packets in priority queue 5. ● Put IP Ping failure attack packets in priority queue 3 and limit the bandwidth for IP packets or the corresponding priority queue.
	Hostname# configure terminal Hostname(config)# cpu-protect type arp traffic-class 1 Hostname(config)# cpu-protect type arp bandwidth 5000 Hostname(config)# cpu-protect type ospf traffic-class 5 Hostname(config)# cpu-protect type v4uc-route traffic-class 3 Hostname(config)# cpu-protect type traffic-class 3 bandwidth 5000 Hostname(config)# end
Verification	Run the **show cpu-protect** command to view the configuration and statistics.
	Hostname#show cpu-protect %cpu port bandwidth: 100000(pps) Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) ------------- -------------- --------- --------- 0 6000 0 0 1 6000 0 0 2 6000 0 0

```
 3              6000            0          0
 4              6000            0          0
 5              6000            0          0
 6              6000            0          0
 7              6000            0          0
Packet Type          Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total          Total
Drop
-------------------  -------------  --------------  ---------  ---------  ---------
----------
bpdu                 6              128             0          0          0              0
arp                  1              3000            0          0          0              0
tpp                  6              128             0          0          0              0
dot1x                2              1500            0          0          0              0
gvrp                 5              128             0          0          0              0
rldp                 5              128             0          0          0              0
lacp                 5              256             0          0          0              0
rerp                 5              128             0          0          0              0
reup                 5              128             0          0          0              0
lldp                 5              768             0          0          0              0
cdp                  5              768             0          0          0              0
dhcps                2              1500            0          0          0              0
dhcps6               2              1500            0          0          0              0
dhcp6-client         2              1500            0          0          0              0
dhcp6-server         2              1500            0          0          0              0
dhcp-relay-c         2              1500            0          0          0              0
dhcp-relay-s         2              1500            0          0          0              0
option82             2              1500            0          0          0              0
tunnel-bpdu          2              128             0          0          0              0
tunnel-gvrp          2              128             0          0          0              0
unknown-v6mc         1              128             0          0          0              0
xgv6-ipmc            1              128             0          0          0              0
stargv6-ipmc         1              128             0          0          0              0
unknown-v4mc         1              128             0          0          0              0
xgv-ipmc             2              128             0          0          0              0
stargv-ipmc          2              128             0          0          0              0
udp-helper           1              128             0          0          0              0
dvmrp                4              128             0          0          0              0
igmp                 2              1000            0          0          0              0
icmp                 3              1600            0          0          0              0
ospf                 4              2000            0          0          0              0
ospf3                4              2000            0          0          0              0
```

	pim	4	1000	0	0	0	0
	pimv6	4	1000	0	0	0	0
	rip	4	128	0	0	0	0
	ripng	4	128	0	0	0	0
	vrrp	6	256	0	0	0	0
	vrrpv6	6	256	0	0	0	0
	ttl0	0	128	0	0	0	0
	ttl1	0	2000	0	0	0	0
	hop-limit	0	800	0	0	0	0
	local-ipv4	3	4000	0	0	0	0
	local-ipv6	3	4000	0	0	0	0
	v4uc-route	1	800	0	0	0	0
	v6uc-route	1	800	0	0	0	0
	rt-host	4	3000	0	0	0	0
	mld	2	1000	0	0	0	0
	nd-snp-ns-na	1	3000	0	0	0	0
	nd-snp-rs	1	1000	0	0	0	0
	nd-snp-ra-redirect	1	1000	0	0	0	0
	erps	5	128	0	0	0	0
	mpls-ttl0	4	128	0	0	0	0
	mpls-ttl1	4	128	0	0	0	0
	mpls-ctrl	4	128	0	0	0	0
	isis	4	2000	0	0	0	0
	bgp	4	2000	0	0	0	0
	cfm	5	512	0	0	0	0
	web-auth	2	2000	0	0	0	0
	fcoe-fip	4	1000	0	0	0	0
	fcoe-local	4	1000	0	0	0	0
	bfd	6	5120	0	0	0	0
	micro-bfd	6	5120	0	0	0	0
	micro-bfd-v6	6	5120	0	0	0	0
	dldp	6	3200	0	0	0	0
	other	0	4096	0	0	0	0
	trill	4	1000	0	0	0	0
	efm	5	1000	0	0	0	0
	ipv6-all	0	2000	0	0	0	0
	ip-option	0	800	0	0	0	0
	mgmt	-	4000	4	0	4639	0
	dns	2	200	0	0	0	0
	sdn	0	5000	0	0	0	0
	sdn_of_fetch	0	5000	0	0	0	0

	sdn_of_copy	0	5000	0	0	0	0
	sdn_of_trap	0	5000	0	0	0	0
	vxlan-non-uc	1	512	0	0	0	0
	local-telnet	3	1000	0	0	0	0
	local-snmp	3	1000	0	0	0	0
	local-ssh	3	1000	0	0	0	0

11.5 Monitoring

Clearing

Description	Command
Clears the CPP statistics.	**clear cpu-protect counters** [**device** *device_num*]
Clears the CPP statistics on the master device.	**clear cpu-protect counters mboard**

Displaying

Description	Command
Displays the configuration and statistics of a packet type.	**show cpu-protect type** *packet-type* [**device** *device_num*]
Displays the configuration and statistics of a priority queue.	**show cpu-protect traffic-class** *traffic-class-num* [**device** *device_num*]
Displays the configuration on a CPU interface.	**show cpu-protect cpu**
Displays all configurations and statistics on the master device.	**show cpu-protect** { **mboard** | **summary** }
Displays all configurations and statistics of CPP.	**show cpu-protect** [**device** *device_num*]

Debugging

N/A

12 Configuring DHCP Snooping

12.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

12.2 Applications

Application	Description
Guarding against DHCP service spoofing	In a network with multiple DHCP servers, DHCP clients are allowed to obtain network configurations only from legal DHCP servers.
Guarding against DHCP packet flooding	Malicious network users may frequently send DHCP request packets.
Guarding against forged DHCP packets	Malicious network users may send forged DHCP request packets, for example, DHCP-RELEASE packets.
Guarding against IP/MAC spoofing	Malicious network users may send forged IP packets, for example, tampered source address fields of packets.
Preventing Lease of IP Addresses	Network users may lease IP addresses rather than obtaining them from a DHCP server.
Detecting ARP attack	Malicious users forge ARP response packets to intercept packets during normal users' communication.

12.2.1 Guarding Against DHCP Service Spoofing

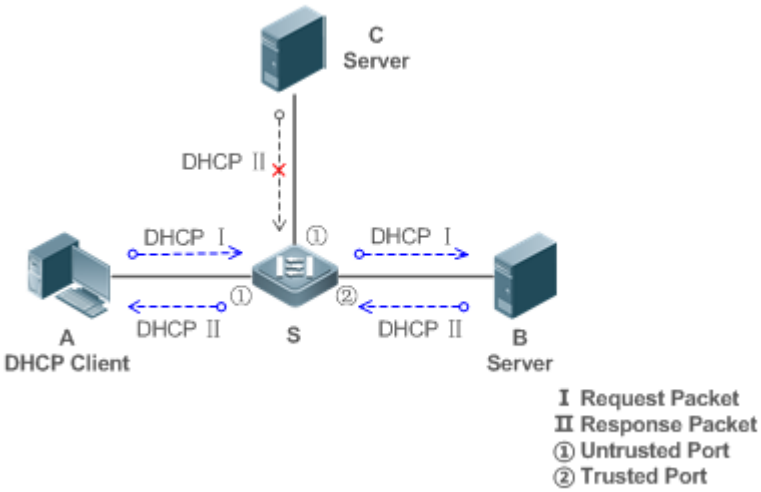
Scenario

Multiple DHCP 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.

Take the following figure as an example. The DHCP client can only communicate with trusted DHCP servers.

- Request packets from the DHCP client can be transmitted only to trusted DHCP servers.
- Only the response packets from trusted DHCP servers can be transmitted to the client.

Figure 12-1



Remarks:	S is an access device. A is a user PC. B is a DHCP server within the controlled area. C is a DHCP server out of the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP packet monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.

12.2.2 Guarding Against DHCP Packet Flooding

Scenario

Potential malicious DHCP clients in a network may send high-rate DHCP packets. As a result, legitimate users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the DHCP Snooping rate limit function for DHCP packets, a DHCP client can only send DHCP request packets at a rate below the limit.

- The request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.
- Enable DHCP Snooping correlation with ARP, and delete the non-existing entries.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.

- Enable DHCP Snooping correlation with ARP, and detect whether the user is online.

12.2.3 Guarding Against Forged DHCP Packets

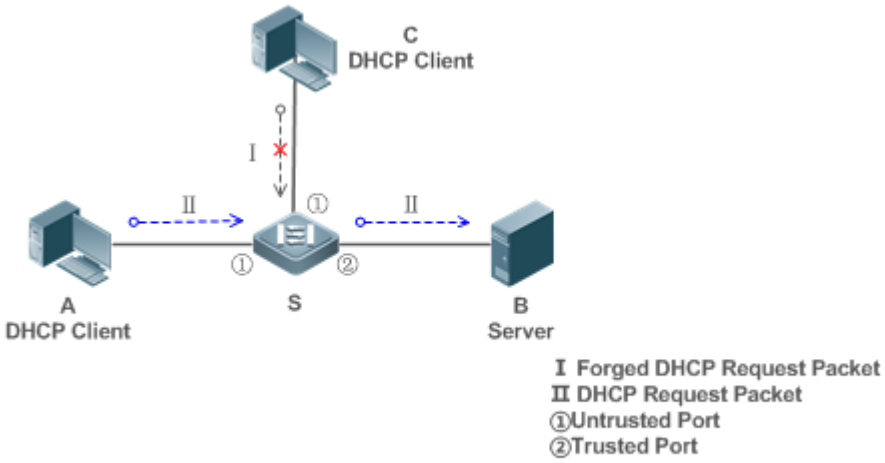
Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addresses from the servers and probably preempting legal users' IP addresses. Therefore, it is necessary to filter out illegal DHCP packets.

For example, as shown in the figure below, the DHCP request packets sent from DHCP clients will be checked.

- The source MAC address fields of the request packets from DHCP clients must match the **chaddr** fields of DHCP packets.
- The Release packets and Decline packets from clients must match the entries in the DHCP Snooping binding database.

Figure 12-2



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.
- Enable DHCP Snooping Source MAC Verification on untrusted ports of S to filter out illegal packets.

12.2.4 Guarding Against IP/MAC Spoofing

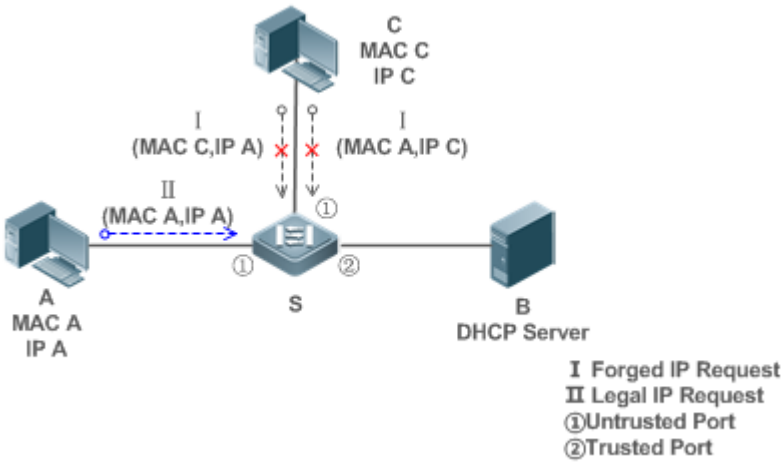
Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP+MAC fields.

For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 12-3



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as DHCP Snooping untrusted.
- Enable IP Source Guard on S to filter IP packets.
- Enable IP Source Guard in IP+MAC based mode to check the source MAC and IP address fields of IP packets.

12.2.5 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

12.2.6 Detecting ARP Attacks

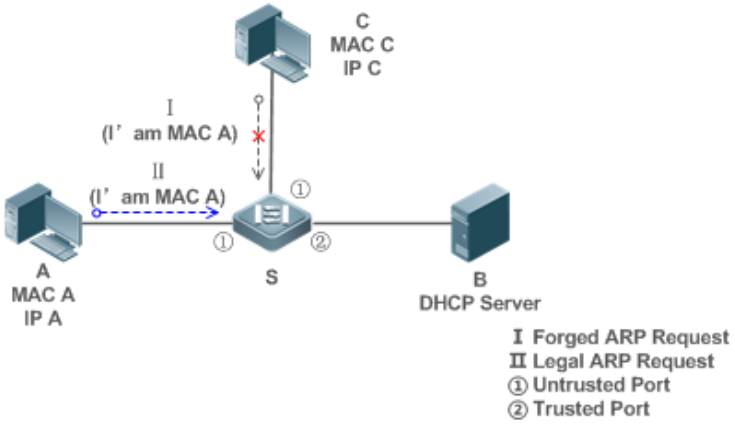
Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP Snooping histories.

Figure 12-4



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as untrusted.
- Enable IP Source Guard and ARP Check on all the untrusted ports on S to realize ARP packet filtering.

All the above security control functions are only effective to DHCP Snooping untrusted ports.

12.3 Features

Basic Concepts

DHCP Request Packets

Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

DHCP Response Packets

Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

DHCP Snooping Trusted Ports

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports. The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified.

DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP Snooping packet suppression on its untrusted ports.

VLAN-based DHCP Snooping

DHCP Snooping can work on a VLAN basis. By default, when DHCP Snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP Snooping flexibly.

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 legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP Snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP Snooping binding database. Combined with ARP detection and ARP check, DHCP Snooping controls the reliable assignment of IP addresses for legal clients.

DHCP Snooping Rate Limit

DHCP Snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay services of a network access device like DHCP Relay and DHCP Snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

Illegal DHCP Packets

Through DHCP Snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP Snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP-ACK, DHCP-NACK and DHCP-OFFER packets
- The DHCP request packets carrying gateway information **giaddr**, which are received on untrusted ports
- When MAC verification is enabled, packets with source MAC addresses different with the value of the **chaddr** field in DHCP packets
- DHCP-RELEASE packets with the entry in the DHCP Snooping binding database Snooping while with untrusted ports inconsistent with settings in this binding database
- DHCP packets in wrong formats, or incomplete

Overview

Feature	Description
Filtering DHCP packets	Perform legality check on DHCP packets and discard illegal packets (see the previous section for the introduction of illegal packets). Transfer requests packets received on trusted ports only.
Building the DHCP Snooping binding database	Snoop the interaction between DHCP clients and the server, and generate the DHCP Snooping binding database to provide basis for other filtering modules.

12.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

Working Principle

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

Checking Ports

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP Snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

Checking Packet Encapsulation and Length

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

Checking Packet Fields and Types

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check whether the restrictive conditions for the type of the packet are met.

Related Configuration

Enabling Global DHCP Snooping

By default, DHCP Snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP Snooping must be enabled before VLAN-based DHCP Snooping is applied.

Configuring VLAN-based DHCP Snooping

By default, when global DHCP Snooping is effective, DHCP Snooping is effective to all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP Snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

Configuring DHCP Snooping Source MAC Verification

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified.

When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP request packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

12.3.2 Building the Binding Database

DHCP Snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP Snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

Generating Binding Entries

When a DHCP-ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index) and VLAN ID. Then, a binding entry of it is generated.

Deleting Binding Entries

When the recorded lease time of a binding entry is due, it will be deleted if a legal DHCP-RELEASE/DHCP-DECLINE packet sent by the client or a DHCP-NCK packet received on a trusted port is snooped, or the **clear** command is used.

Related Configuration

No configuration is needed except enabling DHCP Snooping.

12.4 Configuration

Configuration	Description and Command	
Configuring basic functions of DHCP Snooping	(Mandatory) It is used to enable DHCP Snooping.	
	ip dhcp snooping	Enables DHCP Snooping.
	ip dhcp snooping suppression	Enables DHCP Snooping packet suppression.
	ip dhcp snooping vlan	Enables VLAN-based DHCP Snooping.
	ip dhcp snooping verify mac-address	Configures DHCP Snooping source MAC verification.
	ip dhcp snooping database write-delay	Writes the DHCP Snooping binding database to Flash periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP Snooping binding database to Flash manually.
	renew ip dhcp snooping database	Imports Flash storage to the DHCP Snooping Binding database.
	ip dhcp snooping trust	Configures DHCP Snooping trusted ports.
	ip dhcp snooping bootp	Enables BOOTP support.
	ip dhcp snooping check-giaddr	Enables DHCP Snooping to support the function of processing Relay requests.
	ip dhcp snooping loose-forward	Enables loose forwarding.
Configuring Option82	(Optional)It is used to optimize the address assignment by DHCP servers.	
	ip dhcp snooping Information option	Adds Option82 functions to DHCP request packets.
	ip dhcp snooping information option format remote-id	Configures the sub-potion **remote-id** of Option82 as a user-defined character string.
	ip dhcp snooping vlan information option format-type circuit-id string	Configures the sub-option **circuit-id** of Option82 as a user-defined character string.
	ip dhcp snooping information option strategy	Congifures the strategy of Option82.

12.4.1 Configuring Basic Features

Configuration Effect

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

Notes

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces. The configuration can be implemented in interface configuration mode.
- DHCP Snooping and DHCP Relay are mutually exclusive in VRF scenarios.

Configuration Steps

↘ **Enabling Global DHCP Snooping**

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

↘ **Enabling or Disabling VLAN-based DHCP Snooping**

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

↘ **Configuring DHCP Snooping Trusted Ports**

- Mandatory.
- Configure the ports connecting a trusted DHCP server as trusted.

↘ **Enabling DHCP Snooping Source MAC Validation**

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

↘ **Writing the DHCP Snooping Binding Database to Flash Periodically**

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- Unless otherwise noted, the feature should be configured on access devices.

↘ **Enabling BOOTP Support**

- Optional

- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping to Process Relay Requests

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

Enabling Loose Forwarding

- Optional.
- Unless otherwise noted, the feature is disabled.

Verification

Configure a client to obtain network configurations through the DHCP protocol.

- Check whether the DHCP Snooping Binding database is generated with entries on the client.

Related Commands

Enabling or Disabling DHCP Snooping

Command	[**no**] **ip dhcp snooping**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After global DHCP Snooping is enabled, you can check DHCP Snooping using the **show ip dhcp snooping** command.

Configuring VLAN-based DHCP Snooping

Command	[**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Parameter Description	*vlan-rng*: Indicates the range of VLANs *vlan-min*: The minimum VLAN ID *vlan-max*: The maximum VLAN ID
Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable DHCP Snooping on specified VLANs. This feature is available only after global DHCP Snooping is enabled.

Configuring DHCP Snooping Packet Suppression

Command	[**no**] **ip dhcp snooping suppression**
Parameter Description	N/A
Command	Interface configuration mode

Mode	
Usage Guide	Use this command to reject all DHCP request packets at the port, that is , to forbid all users under the port to apply for addresses via DHCP.

Configuring DHCP Snooping Source MAC Verification

Command	[**no**] **ip dhcp snooping verify mac-address**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Through the source MAC address verification, the MAC addresses in link headers and the CLIENT MAC fields in the request packets sent by a DHCP CLIENT are checked for consistence. When the source MAC address verification fails, packets will be discarded.

Writing DHCP Snooping Database to Flash Periodically

Command	[**no**] **ip dhcp snooping database write-delay** [*time*]
Parameter Description	*time*: Indicates the interval between two times of writing the DHCP Snooping database to the Flash .
Command Mode	Global configuration mode
Usage Guide	Use this command to write the DHCP Snooping database to FLASH document. This can avoid binding information loss which requires re-obtaining IP addresses to resume communication after the device restarts.

Writing the DHCP Snooping Database to Flash Manually

Command	**ip dhcp snooping database write-to-flash**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to write the dynamic user information in the DHCP Snooping database in FLASH documents in real time. If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored from FLASH documents because of version differences between FLASH documents.

Importing Backep File Storage to the DHCP Snooping Binding Database

Command	**renew ip dhcp snooping database**
Parameter Description	N/A
Command	Privileged configuration mode

Mode	
Usage Guide	Use this command to import the information from backup file to the DHCP Snooping binding database.

Configuring DHCP Snooping Trusted Ports

Command	[**no**] **ip dhcp snooping trust**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a port connected to a legal DHCP server as a trusted port. The DHCP response packets received by trusted ports are transferred, while those received by untrusted ports are discarded.

Enabling or Disabling BOOTP Support

Command	[**no**] **ip dhcp snooping bootp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOPT protocol.

Enabling DHCP Snooping to Process Relay Requests

Command	[**no**] **ip dhcp snooping check-giaddr**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet. After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

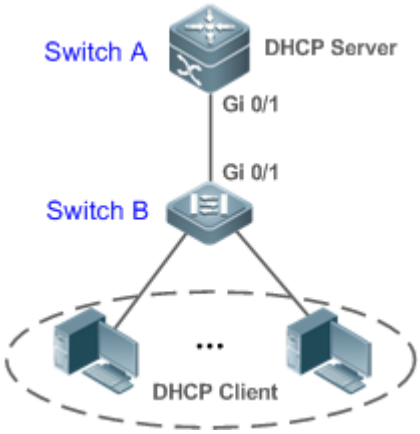
Enabling DHCP Snooping Loose Forwarding

Command	**ip dhcp snooping loose-forward**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this feature is enabled, when the capacity of DHCP Snooping binding entries is reached, DHCP

	packets of new users are forwarded and obtain addresses, but DHCP Snooping does not record binding entries of new users.

Configuration Example

DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Scenario **Figure 12-5**	
Configuration Steps	● Enable DHCP Snooping on an access device (Switch B in this case). ● Configure the uplink port (port Gi 0/1 in this case) as a trusted port.
B	B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ip dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end
Verification	Check the configuration on Switch B. ● Check whether DHCP Snooping is enabled, and whether the configured DHCP Snooping trusted port is uplink. ● Check the DHCP Snooping configuration on Switch B, and especially whether the trusted port is correct.
B	B#show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr 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
B#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress         IpAddress       Lease(sec)   Type          VLAN  Interface
------------------ --------------- ------------ ------------- ----- --------------------
0013.2049.9014     172.16.1.2      86207        DHCP-Snooping 1     GigabitEthernet 0/11
```

Common Errors

- The uplink port is not configured as a DHCP trusted port.
- Another access security option is already configured for the uplink port, so that a DHCP trusted port cannot be configured.

12.4.2 Configuring Option82

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Opion82 functions for DHCP Snooping and DHCP Relay are mutually exclusive.

Configuration Steps

- To realize optimization of address allocation, implement the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP Snooping enabled.

Verification

Check whether the DHCP Snooping configuration options are configured successfully.

Related Commands

Adding Option82 to DHCP Request Packets

Command	[**no**] **ip dhcp snooping information option** [**standard-format** | **dot1x-format**]
Parameter Description	**standard-format**: Indicates a standard format of the Option82 options **dot1x-format**: Indicates a dot1x format of the Option82 options
Command Mode	Global configuration mode

Usage Guide	Use this command to add Option82 to DHCP request packets so that a DHCP server assigns addresses according to such information. When dot1x-format is used, if DHCP Relay is configured on the local device and the uplink port connected to the DHCP Server is an SVI port, DHCP Snooping needs to be disabled in the VLAN to which the SVI port belongs.

Configuring Sub-option remote-id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Parameter Description	**string** *ASCII-string*: Indicates the content of the extensible format, the Option82 option **remote-id**, is a user-defined character string **hostname**: Indicates the content of the extensible format, the Option82 option **remote-id**, is a host name.
Configuration mode	Global configuration mode
Usage Guide	Use this command to configure the sub-option **remote-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuring Sub-Option circuit -id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*
Parameter Description	*vlan-id*: Indicates the VLAN where a DHCP request packet is *ascii-string*: Indicates the user-defined string
Configuration mode	Interface configuration mode
Usage Guide	Use this command to configure the sub-option **circuit-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuring the Strategy of Option82

Command	**ip dhcp snooping information option strategy {keep | drop | replace}**
Parameter Description	**keep:** Indicates reception of request packets with Option82. Option82 is kept and the packets are forwarded. **drop:** Indicates reception of request packets with Option82. The packets are dropped. **replace: I**ndicates reception of request packets with Option82. Option82 of the packets are replaced with Option82 configured latest. The packets are forwarded.
Configuration mode	Global configuration mode
Usage Guide	This command only works for request packets with Option82. If the strategy is keep or drop, there is no need to configure sub-option **circuit-id** of the Option82. If the strategy is replace, sub-option **circuit-id** of the Option82 needs configuring. In terms of request packets without Option82, configured sub-option **circuit-id** of the Option82 is added.

Configuration Example

Configuring Option82 to DHCP Request Packets

Configuration Steps	● Configuring basic functions of DHCP Snooping. ● Configuring Option82.
B	Hostname# configure terminal Hostname(config)# ip dhcp snooping information option Hostname(config)# end
Verification	Check the DHCP Snooping configuration.
B	B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : ENABLE DHCP Snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ------------------------ ------- ---------------- GigabitEthernet 0/1 YES unlimited

Common Errors

- N/A

12.5 Monitoring

Clearing

⚠ Running the clear commands maylose vital information and thus interrupt services.

Description	Command
Clears dynamic user inforamtion of DHCP Snooping database.	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

Displaying

Description	Command
Displays DHCP Snooping configuration.	**show ip dhcp snooping**
Displays the DHCP Snooping binding database.	**show ip dhcp snooping binding**

Debugging

⚠ System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs DHCP Snooping events.	**debug snooping ipv4 event**
Disables debugging DHCP Snooping events.	**no debug snooping ipv4 event**
Debugs DHCP Snooping packets.	**debug snooping ipv4 packet**
Disables debugging DHCP Snooping packets.	**no debug snooping ipv4 packet**
Enables debugging MAC-based DHCP Snooping.	**debug snooping ipv4 mac-address** *H.H.H*
Disables debugging MAC-based DHCP Snooping.	**no debug snooping ipv4 mac-address** *H.H.H*
Enables debugging all DHCP Snooping	**debug snooping ipv4 all**
Disables debugging all DHCP Snooping	**no debug snooping ipv4 all**

13 Configuring Dynamic ARP Inspection

13.1 Overview

Dynamic Address Resolution Protocol (ARP) inspection (DAI) checks the validity of received ARP packets. Invalid ARP packets will be discarded.

DAI ensures that only valid ARP packets can be forwarded by devices. DAI mainly performs the following steps:

- Intercepts all ARP request packets and ARP reply packets on untrusted ports in the virtual local area networks (VLANs) where the DAI function is enabled.
- Checks the validity of intercepted ARP packets according to user records stored in a security database.
- Discards the ARP packets that do not pass the validity check.
- Sends the ARP packets that pass the validity check to the destination.
- The DAI validity criteria are the same as those of ARP Check. For details, see the *Configuring ARP Check*.

DAI and ARP Check have same functions. The only difference is that DAI takes effect by VLAN whereas ARP Check takes effect by port.

Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

13.2 Applications

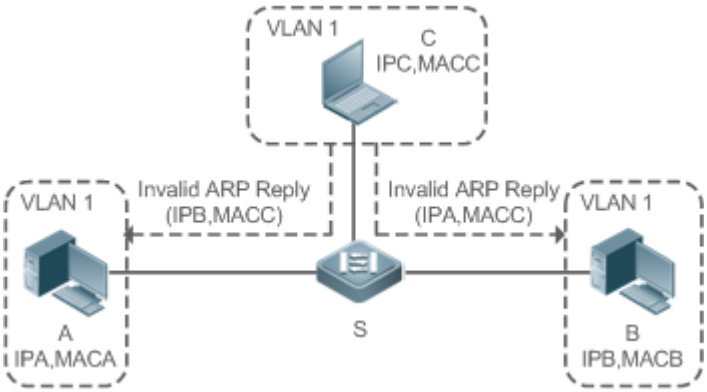
Application	Description
ARP Spoofing Prevention	Prevent ARP spoofing that is mounted by taking advantage of ARP defects.

13.2.1 ARP Spoofing Prevention

Scenario

Due to inherent defects, ARP does not check the validity of received ARP packets. Attackers can take advantage of the defects to mount ARP spoofing. A typical example is man-in-the-middle (MITM) attack. See Figure 13-1.

Figure 13-1



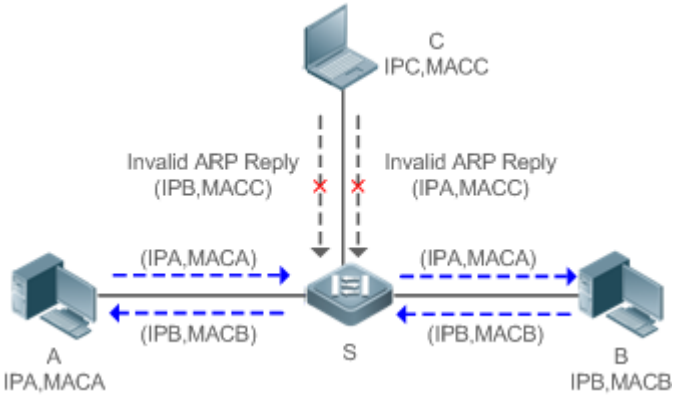
Remarks	Device S is a Hostname access switch enabled with DAI. User A and User B are connected to Device S, and they are in the same subnet. User C is a malicious user connected to Device S. IP A and MAC A are the IP address and MAC address of User A. IP B and MAC B are the IP address and MAC address of User B. IP C and MAC C are the IP address and MAC address of User C.

When User A needs to initiate network layer communication with User B, User A broadcasts an ARP request in the subnet to query the MAC address of User B. Upon receiving the ARP request packet, User B updates its ARP cache with IP A and MAC A, and sends an ARP reply. Upon receiving the ARP reply packet, User A updates its ARP cache with IP B and MAC B.

In this model, User C can make the ARP entry mapping between User A and User B incorrect by continuously broadcasting ARP reply packets to the network. The reply packets contain IP A, IP B, and MAC C, After receiving these reply packets, User A stores the ARP entry (IP B, MAC C), and User B stores the ARP entry (IP A, MAC C). As a result, the communication between User A and User B is directed to User C, without the knowledge of User A and User B. Here User C acts as the man in the middle by modifying received packets and forwarding them to User A or User B.

If Device S is enabled with DAI, it will filter out forged ARP packets to prevent ARP spoofing as long as the IP addresses of User A and User B meet the validity criteria described in section 13.1 Overview. Figure 13-2 shows the working process of DAI.

Figure 13-2



Remarks	Device S is a Hostname access switch enabled with DAI. User A and User B are connected to Device S, and they are in the same subnet. User C is a malicious user connected to Device S. IP A and MAC A are the IP address and MAC address of User A. IP B and MAC B are the IP address and MAC address of User B. IP C and MAC C are the IP address and MAC address of User C.

The ARP packets of User A and User B are forwarded normally by Device S. The forged ARP packets of User C are discarded because the packets do not match the records in the security database of Device S.

Deployment

- Enable DHCP Snooping on Device S.
- Enable DAI and IP Source Guard on Device S.

13.3 Features

Basic Concepts

Trust Status of Ports and Network Security

ARP packet check is performed according to the trust status of ports. DAI considers packets received from trusted ports as valid without checking their validity, but it checks the validity of packets received from untrusted ports.

For a typical network configuration, you should configure Layer-2 ports connected to network devices as trusted ports, and configure Layer-2 ports connected to hosts as untrusted ports.

Network communication may be affected if a Layer-2 port connected to a network device is configured as an untrusted port.

Overview

Feature	Description
Invalid ARP Packet Filter	Checks the source IP addresses and MAC addresses of ARP packets to filter out invalid packets.
DAI Trusted Port	Permits the ARP packets received from specific ports to pass through without checking their validity.

13.3.1 Invalid ARP Packet Filter

Enable DAI in a specific VLAN to filter out invalid ARP packets. The DAI validity criteria are the same as those of ARP Check.

Working Principle

Upon receiving an ARP packet, the device matches the IP address and MAC address of the packet with the valid user records in its security database. If the packet matches a record, it will be forwarded normally. If it does not match any record, it will be discarded.

DAI and ARP Check use the same set of valid user records. For details, see the packet validity check description in the *Configuring ARP Check*.

Related Configuration

Enabling DAI in a VLAN

By default, DAI is disabled in VLANs.

Run the **ip arp inspection vlan** *vlan-id* command to enable DAI in a specific VLAN.

After DAI is enabled in a VLAN, DAI may not take effect on all ports in the VLAN. A DHCP Snooping trusted port does not perform DAI check.

Disabling DAI in a VLAN

By default, DAI is disabled in VLANs.

After DAI is enabled in a VLAN, you can run the **no ip arp inspection vlan** *vlan-id* command to disable DAI.

Disabling DAI in a VLAN does not mean disabling packet validity check on all ports in the VLAN. The ports with ARP Check effective still check the validity of received ARP packets.

13.3.2 DAI Trusted Port

Configure specific device ports as DAI trusted ports.

Working Principle

The validity of ARP packets received from trusted ports is not checked. The ARP packets received from untrusted ports are checked against the user records in a security database.

Related Configuration

Configuring DAI Trusted Ports

By default, all ports are untrusted ports.

Run the **ip arp inspection trust** command to set ports to trusted state.

A port already enabled with access security control cannot be set to DAI trusted state. To set the port to DAI trusted state, first disable access security control.

In normal cases, uplink ports (ports connected to network devices) can be configured as DAI trusted ports.

13.4 Configuration

Configuration	Description and Command	
Configuring DAI	(Optional) It is used to enable ARP packet validity check.	
	ip arp inspection vlan	Enables DAI.
	ip arp inspection trust	Configures DAI trusted ports.

13.4.1 Configuring DAI

Configuration Effect

- Check the validity of incoming ARP packets in a specific VLAN.

Notes

- DAI cannot be enabled on DHCP Snooping trusted ports.

Configuration Steps

Enabling ARP Packet Validity Check in a Specific VLAN

- Optional.
- Perform this configuration when you need to enable ARP packet validity check on all ports in a VLAN.
- Perform this configuration on Hostname access devices unless otherwise specified.

Configuring DAI Trusted Ports

- Optional.
- It is recommended to configure uplink ports as DAI trusted ports after DAI is enabled. Otherwise, the uplink ports enabled with other security features and set to trusted state accordingly may filter out valid ARP packets due to the absence of DAI user entries.
- Perform this configuration on Hostname access devices unless otherwise specified.

Configuring the ARP Packet Reception Rate

- For details, see the rate limit command description in the *Configuring the NFPP*.

Verification

- Construct invalid ARP packets by using a packet transfer tool and check whether the packets are filtered out on DAI-enabled devices.
- Run the **show** command to check the device configuration.

Related Commands

Enabling DAI

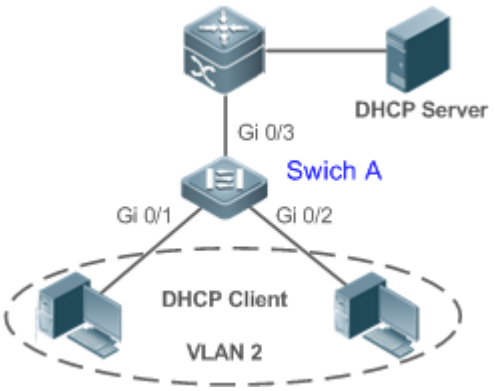
Command	**ip arp inspection vlan** { *vlan-id* | *word* }
Parameter Description	*vlan-id*: Indicates a VLAN ID. *word*: Indicates the VLAN range string, such as 1, 3–5, 7, and 9–11.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring DAI Trusted Ports

Command	**ip arp inspection trust**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a DAI trusted port so that the ARP packets received by the port can pass through without validity check.

Configuration Example

Allowing Users' PCs to Use only Addresses Allocated by a DHCP Server to Prevent ARP Spoofing

Scenario **Figure 13-3**	
Configuration Steps	Enable DHCP Snooping on the access switch (Switch A) and configure its uplink port (GigabitEthernet 0/3) connected to the valid DHCP server as a trusted port. Enable IP Source Guard on Switch A. Enable DAI.
Switch A	A#configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)#vlan 2

	A(config-vlan)#exit A(config)#interface range gigabitEthernet 0/1-2 A(config-if-range)#switchport access vlan 2 A(config-if-range)#ip verify source A(config-if-range)#exit A(config)#ip dhcp snooping A(config)#ip arp inspection vlan 2 A(config)#interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport access vlan 2 A(config-if-GigabitEthernet 0/3)#ip dhcp snooping trust A(config-if-GigabitEthernet 0/3)#ip arp inspection trust
Verification	● Check whether DHCP Snooping, IP Source Guard, and DAI are enabled and whether trusted ports are configured correctly. ● Check whether the uplink port on Switch A is a DHCP Snooping trusted port. ● Check whether DAI is enabled successfully in the VLAN and the uplink ports are DAI trusted ports.
Switch A	A#show running-config A#show ip dhcp snooping A#show ip arp inspection vlan

Common Errors

- A port with security control enabled is configured as a DAI trusted port.

13.5 Monitoring

Displaying

Description	Command
Displays the DAI state of a specific VLAN.	**show ip arp inspection vlan** [*vlan-id* | *word*]
Displays the DAI configuration state of each Layer-2 port.	**show ip arp inspection interface**

14 Configuring IP Source Guard

14.1 Overview

The IP Source Guard function realizes hardware-based IP packet filtering to ensure that only the users having their information in the binding database can access networks normally, preventing users from forging IP packets.

14.2 Applications

Application	Description
Guarding Against IP/MAC Spoofing Attack	In network environments, users set illegal IP addresses and malicious users launch attacks through forging IP packets.

14.2.1 Guarding Against IP/MAC Spoofing Attack

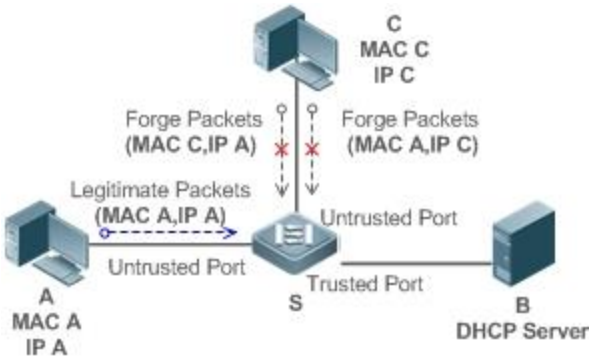
Scenario

Check the IP packets from DHCP untrusted ports. Forged IP packets will be filtered out based on the IP or IP-MAC field.

For example, in the following figure, the IP packets sent by DHCP clients are checked.

- The Source IP Address fields of IP packets should match DHCP-assigned IP addresses.
- The Source MAC Address fields of layer-2 packets should match the MAC addresses in DHCP request packets from clients.

Figure 14-1



Remarks:	S is a network access server (NAS). A and C are user PCs. B is a DHCP server within the control area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on S as DHCP untrusted ports.
- Enable IP Source Guard on S to realize IP packet filtering.
- Enable IP–MAC match mode for IP Source Guard on S, filtering IP packets based on IP and MAC addresses.

14.3 Features

Basic Concepts

Source IP Address

Indicate the source IP address field of an IP packet.

Source MAC Address

Indicate the source MAC address field of an IP packet.

IP-based Filtering

Indicate a policy of IP packet filtering, where only the source IP addresses of all IP packets (except DHCP packets) passing through a port are checked. It is the default filtering policy of IP Source Guard.

IP-MAC based Filtering

A policy of IP packet filtering, where both the source IP addresses and source MAC addresses of all IP packets are checked, and only those user packets with these IP addresses and MAC addresses existing in the binding database are permitted.

Address Binding Database

As the basis of security control of the IP Source Guard function, the data in the address binding database comes from two ways: the DHCP Snooping binding database and static configuration. When IP Source Guard is enabled, the data of the DHCP Snooping binding database is synchronized to the address binding database of IP Source Guard, so that IP packets can be filtered strictly through IP Source Guard on a device with DHCP Snooping enabled.

Excluded VLAN

By default, when IP Source Guard is enabled on a port, it is effective to all the VLANs under the port. Users may specify excluded VLANs, within which IP packets are not checked and filtered, which means that such IP packets are not controlled by IP Source Guard. At most 32 excluded VLANs can be specified for a port.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter the IP packets passing through ports by IP-based or IP-MAC based filtering.

14.3.1 Checking Source Address Fields of Packets

Filter the IP packets passing through ports based on source IP addresses or on both source IP addresses and source MAC addresses to prevent malicious attack by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to release such packets.

Working Principle

When IP Source Guard is enabled, the source addresses of packets passing through a port will be checked. The port can be a wired switching port, a layer-2 aggregate port (AP), or a layer-2 encapsulation sub-interface. Such packets will pass the port only when the source address fields of the packets match the set of the address binding records generated by DHCP Snooping, or the static configuration set by the administrator. There are two matching modes as below.

IP-based Filtering

Packets are allowed to pass a port only if the source IP address fields of them belong to the address binding database.

IP-MAC Based Filtering

Packets are allowed to pass a port only when both the layer-2 source MAC addresses and layer-3 source IP addresses of them match an entry in the address binding database.

Specifying Excluded VLAN

Packets within such a VLAN are allowed to pass a port without check or filtering.

Related Configuration

Enabling IP Source Guard on a Port

By default, the IP Source Guard is disabled on ports.

It can be enabled using the **ip verify source** command.

Usually IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled. DHCP Snooping can be enabled at any time on Hostname devices, either before or after IP Source Guard is enabled.

Configuring a Static Binding

By default, legal users passing IP Source Guard check are all from the binding database of DHCP Snooping.

Bound users can be added using the **ip source binding** command.

Specifying an Excluded VLAN

By default, IP Source Guard is effective to all the VLANs under a port.

Excluded VLANs may be specified which are exempted from IP Source Guard using the **ip verify source exclude-vlan** command.

Excluded VLANs can be specified only after IP Source Guard is enabled on a port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on a port.

The above-mentioned port can be a wired switching port, a layer-2 AP port or a layer-2 encapsulation sub-interface.

14.4 Configuration

Configuration	Description and Command	
Configuring IP Source Guard	(Mandatory) It is used to enable IP Source Guard.	
	ip verify source	Enables IP Source Guard on a port.
	ip source binding	Configures a static binding.
	Ip verify source exclude-vlan	Specifies an excluded VLAN for IP Source Guard.

14.4.1 Configuring IP Source Guard

Configuration Effect

- Check the source IP addresses of input IP packets.

Notes

- When IP Source Guard is enabled, IP packets forwarding may be affected. In general case, IP Source Guard is enabled together with DHCP Snooping.
- IP Source Guard cannot be configured on the trusted ports controlled by DHCP Snooping.
- IP Source Guard cannot be configured on the global IP+MAC exclusive ports.
- IP Source Guard can be configured and enabled only on wired switch ports, Layer-2 AP ports and Layer-2 encapsulation sub-ports. In a wired access scenario, it is supposed to be configured in the interface configuration mode.

Configuration Steps

- Enable DHCP Snooping.
- Enable IP Source Guard.

Verification

Use the monitoring commands to display the address binding database of IP Source Guard.

Related Commands

Enabling IP Source Guard on a Port

Command	**ip verify source** [**port-security**]
Parameter Description	**port-security**: Enable IP-MAC based filtering.
Command	Interface configuration mode

Usage Guide	Detection of users based on IP address or both IP and MAC addresses can be realized by enabling IP Source Guard for a port.

Configuring a Static Binding

Command	**ip source binding** *mac-address* **{ vlan** *vlan-id* **}** *ip-address* **{ interface** *interface-id* **| ip-mac | ip-only }**
Parameter Description	*mac-address:* The MAC address of a static binding *vlan-id:* The VLAN ID of a static binding. It indicates the outer VLAN ID of a QINQ-termination user. **ip-address:** The IP address of a static binding *interface-id*: The Port ID (PID) of a static binding **ip-mac:** IP-MAC based mode **ip-only:** IP-based mode
Configuration Mode	Global configuration mode
Usage Guide	Through this command, legitimate users can pass IP Source Guard detection instead of being controlled by DHCP.

Specifying an Exception VLAN for IP Source Guard

Command	**ip verify source exclude-vlan** *vlan-id*
Parameter Description	**vlan-id:** A VLAN ID exempted from IP Source Guard on a port
Command	Interface configuration mode
Usage Guide	By using this command, the specified VLANs under a port where IP Source Guard function is enabled can be exempted from check and filtering.

Configuration Example

Enabling IP Source Guard on Port 1

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.

	`Hostname(config)# interface GigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# ip verify source`
	`Hostname(config-if-GigabitEthernet 0/1)# end`

Verification	Displays the address filtering table of IP Source Guard.
	`Hostname# show ip verify source`

Configuring a Static Binding

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard. ● Configure a static binding.
	Hostname# configure terminal Hostname(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3 Hostname(config)# end
Verification	Displays the address filtering table of IP Source Guard.
	Hostname# show ip verify source NO. INTERFACE FilterType FilterStatus IPADDRESS MACADDRESS VLAN TYPE ----- ---------- ---------- ---------- ---------- ---------- ---- ---------- 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 Static 2 GigabitEthernet 0/1 IP-ONLY Active Deny-All

Specifying an Excluded VLAN

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.
	Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip verify source Hostname(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 Hostname(config-if)# end
Verification	Displaythe configuration of excluded VLANs specified on a port.
	Hostname# show run

Common Errors

- Enable IP Source Guard on a trusted port under DHCP Snooping.
- Specify an excluded VLAN before IP Source Guard is enabled.

14.5 Monitoring

Displaying

Description	Command
Displays the address filtering table of IP Source Guard.	**show ip verify source** [**interface** *interface-id*]
Displays the address binding database of IP Source Guard.	**show ip source binding**

15 Configuring NFPP

15.1 Overview

Network Foundation Protection Policy (NFPP) provides guards for switches.

Malicious attacks are always found in the network environment. These attacks bring heavy burdens to switches, resulting in high CPU usage and operational troubles. These attacks are as follows:

Denial of Service (DoS) attacks may consume lots of memory, entries, or other resources of a switch, which will cause system service termination.

Massive attack traffic is directed to the CPU, occupying the entire bandwidth of the CPU. In this case, normal protocol traffic and management traffic cannot be processed by the CPU, causing protocol flapping or management failure. The forwarding in the data plane will also be affected and the entire network will become abnormal.

A great number of attack packets directed to the CPU consume massive CPU resources, making the CPU highly loaded and thereby influencing device management and performance.

NFPP can effectively protect the system from these attacks. Facing attacks, NFPP maintains the proper running of various system services with a low CPU load, thereby ensuring the stability of the entire network.

15.2 Applications

Application	Description
Attack Rate Limiting	Due to various malicious attacks such as ARP attacks and IP scanning attacks in the network, the CPU cannot process normal protocol and management traffics, causing protocol flapping or management failure. The NFPP attack rate limiting function is used to limit the rate of attack traffic or isolate attack traffic to recover the network.
CentralizedBandwidth Allocation	If normal service traffics are too large, you need to classify and prioritize the traffics. When a large number of packets are directed to the CPU, the CPU will be highly loaded, thereby causing device management or device running failure. The centralized bandwidth distribution function is used to increase the priority of such traffics so that switches can run stably.

15.2.1 Attack Rate Limiting

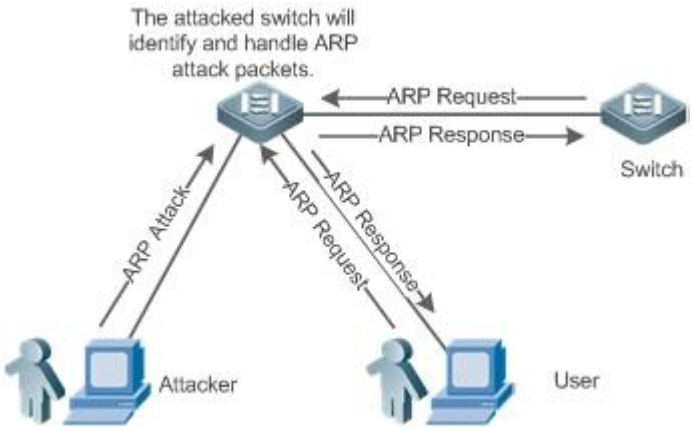
Scenario

NFPP supports attack detection and rate limiting for various types of packets, including Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Dynamic Host Configuration Protocol (DHCP) packets. It also allows users to define packet matching characteristics and corresponding attack detection and rate limiting policies. The attack rate limiting

function takes effect based on types of packets. This section uses ARP packets as an example scenario to describe the application.

If an attacker floods ARP attack packets while CPU capability is insufficient, most of the CPU resources will be consumed for processing these ARP packets. If the rate of attacker's ARP packet rates exceeds the maximum ARP bandwidth specified in the CPU Protect Policy (CPP) of the switch, normal ARP packets may be dropped. As shown in Figure 15-1, normal hosts will fail to access the network, and the switch will fail to send ARP replies to other devices.

Figure 15-1



Deployment

- By default, the ARP attack detection and rate limiting function is enabled with corresponding policies configured. If the rate of an attacker's ARP packets exceeds the rate limit, the packets are discarded. If it exceeds the attack threshold, a monitoring user is generated and prompt information is exported.
- If the rate of an attacker's ARP packets exceeds the rate limit defined in CPP and affects normal ARP replies, you can enable attack isolation to discard ARP attack packets based on the hardware and recover the network.

For details about CPP-related configurations, see the *Configuring CPU Protection*.

To maximize the use of NFPP guard functions, modify the rate limits of various services in CPP based on the application environment or use the configurations recommended by the system. You can run the **show cpu-protect summary** command to display the configurations.

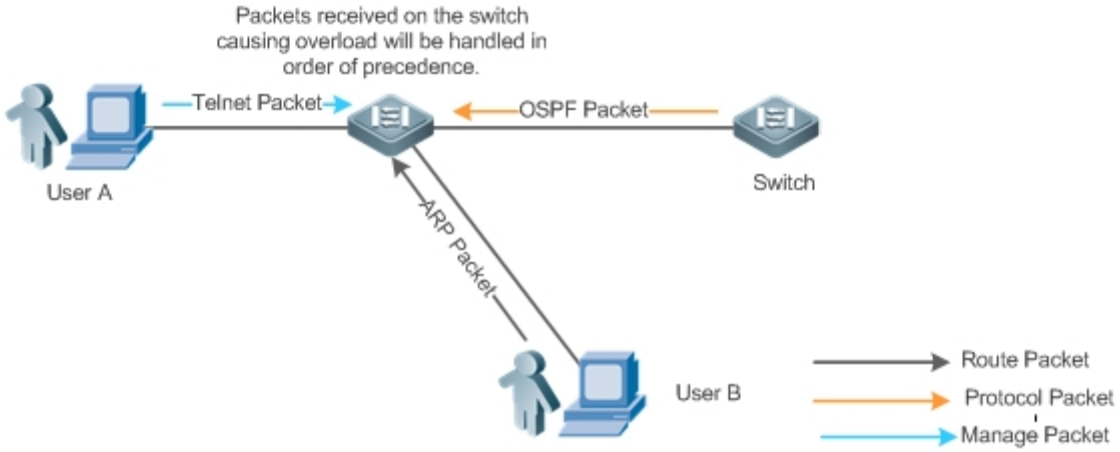
15.2.2 Centralized Bandwidth Allocation

Scenario

A switch classifies services defined in CPP into three types: Manage, Route, and Protocol. Each type of services has an independent bandwidth. Different types of services cannot share their bandwidths. Traffics with bandwidths exceeding the thresholds will be discarded. By such service classification, service packets are processed by orders of precedence.

As shown in Figure 15-2, the switch receives a large number of Telnet packets, OSPF packets, and ARP packets, causing CPU overload. In this case, the CPU cannot process all packets, and a large quantity of packets are backlogged in the queue, causing various problems such as frequent Telnet disconnection, OSPF protocol flapping, and ARP access failure on hosts.

Figure 15-2



Deployment

- By default, CPU centralized bandwidth allocation is enabled to assign an independent bandwidth and bandwidth ratio to each type of services. At the time, the CPU first processes Telnet packets to ensure uninterrupted connection of Telnet service, and then processes OSPF packets to maintain OSPF protocol stability, and finally processes ARP packets.
- If the preceding problems still occur in default configurations, you can accordingly adjust the bandwidths and bandwidth ratios of various types of services.

15.3 Features

Basic Concepts

↘ ARP Guard

In local area networks (LANs), IP addresses are mapped to MAC addresses through ARP, which has a significant role in safeguarding network security. ARP-based DoS attacks mean that a large number of unauthorized ARP packets are sent to the gateway through the network, causing the failure of the gateway to provide services for normal hosts. To prevent such attacks, limit the rate of ARP packets and identify and isolate the attack source.

↘ IP Guard

Many hacker attacks and network virus intrusions start from scanning active hosts in the network. Therefore, many scanning packets rapidly occupy the network bandwidth, causing network communication failure.

To solve this problem, Hostname Layer-3 switches provide IP guard function to prevent hacker scanning and Blaster Worm viruses and reduce the CPU load. Currently, there are mainly two types of IP attacks:

Scanning destination IP address changes: As the greatest threat to the network, this type of attacks not only consumes network bandwidth and increases device load but also is a prelude of most hacker attacks.

Sending IP packets to non-existing destination IP addresses at high rates: This type of attacks is mainly designed for consuming the CPU load. For a Layer-3 device, if the destination IP address exists, packets are directly forwarded by the switching chip without occupying CPU resources. If the destination IP address does not exist, IP packets are sent to the CPU, which then sends ARP requests to query the MAC address corresponding to the destination IP address. If too many packets are sent to the CPU, CPU resources will be consumed. This type of attack is less destructive than the former one.

To prevent the latter type of attack, limit the rate of IP packets and find and isolate the attack source.

↘ ICMP Guard

ICMP is a common approach to diagnose network failures. After receiving an ICMP echo request from a host, the router or switch returns an ICMP echo reply. The preceding process requires the CPU to process the packets, thereby definitely consuming part of CPU resources. If an attacker sends a large number of ICMP echo requests to the destination device, massive CPU resources on the device will be consumed heavily, and the device may even fail to work properly. This type of attacks is called ICMP flood. To prevent this type of attacks, limit the rate of ICMP packets and find and isolate the attack source.

↘ DHCP Guard

DHCP is widely used in LANs to dynamically assign IP addresses. It is significant to network security. Currently, the most common DHCP attack, also called DHCP exhaustion attack, uses faked MAC addresses to broadcast DHCP requests. Various attack tools on the Internet can easily complete this type of attack. A network attacker can send sufficient DHCP requests to use up the address space provided by the DHCP server within a period. In this case, authorized hosts will fail to request DHCP IP addresses and thereby fail to access the network. To prevent this type of attacks, limit the rate of DHCP packets and find and isolate the attack source.

↘ DHCPv6 Guard

DHCP version 6 (DHCPv6) is widely used in LANs to dynamically assign IPv6 addresses. Both DHCP version 4 (DHCPv4) and DHCPv6 have security problems. Attacks to DHCPv4 apply also to DHCPv6. A network attacker can send a large number of DHCPv6 requests to use up the address space provided by the DHCPv6 server within a period. In this case, authorized hosts will fail to request IPv6 addresses and thereby fail to access the network. To prevent this type of attacks, limit the rate of DHCPv6 packets and find and isolate the attack source.

↘ ND Guard

Neighbor Discovery (ND) is mainly used in IPv6 networks to perform address resolution, router discovery, prefix discovery, and redirection. ND uses five types of packets: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect. These packets are called ND packets.

↘ Self-Defined Guard

There are various types of network protocols, including routing protocols such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). Various devices need to exchange packets through different protocols. These packets must be sent to the CPU and processed by appropriate protocols. Once the network device runs a protocol, it is like opening a window for attackers. If an attacker sends a large number of protocol packets to a network device, massive CPU resources will be consumed on the device, and what's worse, the device may fail to work properly.

Since various protocols are being continuously developed, protocols in use vary with the user environments. Hostname devices hereby provide self-defined guard. Users can customize and flexibly configure guard types to meet guard requirements in different user environments.

Overview

Feature	Description
Host-based Rate Limiting and Attack Identification	Limits the rate according to the host-based rate limit and identify host attacks in the network.
Port-based Rate Limiting and Attack Identification	Limits the rate according to the port-based rate limit and identify port attacks.
Monitoring Period	Monitors host attackers in a specified period.
Isolation Period	Uses hardware to isolate host attackers or port attackers in a specified period.
Trusted Hosts	Trusts a host by not monitoring it.
Centralized BandwidthAllocation	Classifies and prioritizes packets.

15.3.1 Host-based Rate Limiting and Attack Identification

Limit the rate of attack packets of hosts and identify the attacks.

Identify ARP scanning.

Identify IP scanning.

Working Principle

Hosts can be identified in two ways: based on the source IP address, VLAN ID, and port and based on the link-layer source MAC address, VLAN ID, and port. Each host has a rate limit and an attack threshold (also called alarm threshold). The rate limit must be lower than the attack threshold. If the attack packet rate exceeds the rate limit of a host, the host discards the packets beyond the rate limit. If the attack packet rate exceeds the attack threshold of a host, the host identifies and logs the host attacks, and sends traps.

ARP scanning attack may have occurred if ARP packets beyond the scanning threshold received in the configured period meet either of the following conditions:

- The link-layer source MAC address is fixed but the source IP address changes.
- The link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes.

Among IP packets beyond the scanning threshold received in the configured period, if the source IP address remains the same while the destination IP address continuously changes, IP scanning attack may have occurred.

When NFPP detects a specific type of attack packets under a service, it sends a trap to the administrator. If the attack traffic persists, NFPP will not resend the alarm until 60 seconds later.

To prevent CPU resource consumption caused by frequent log printing, NFPP writes attack detection logs to the buffer, obtains them from the buffer at a specified rate, and prints them. NFPP does not limit the rate of traps.

Related Configuration

Use ARP guard as an example:

Configuring the Global Host-based Rate Limit, Attack Threshold, and Scanning Threshold

In NFPP configuration mode:

Run the **arp-guard rate-limit** {**per-src-ip** | **per-src-mac**} *pps* command to configure rate limits of hosts identified based on the source IP address, VLAN ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port.

Run the **arp-guard attack-threshold** {**per-src-ip** | **per-src-mac**} *pps* command to configure attack thresholds of hosts identified based on the source IP address, VLAN ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port.

Run the **arp-guard scan-threshold** *pkt-cnt* command to configure the ARP scanning threshold.

Configuring Host-based Rate Limit and Attack Threshold, and Scanning Threshold on an Interface

In interface configuration mode:

Run the **nfpp arp-guard policy** {**per-src-ip | per-src-mac**} *rate-limit-pps attack-threshold-pps* command to configure rate limits and attack thresholds of hosts identified based on the source IP address, VLAN ID, and port and hosts identified based on the link-layer source MAC address, VLAN ID, and port on an interface.

Run the **nfpp arp-guard scan-threshold** *pkt-cnt* command to configure the scanning threshold on an interface.

Only ARP guard and IP guard support anti-scanning at present.

15.3.2 Port-based Rate Limiting and Attack Identification

Working Principle

Each port has a rate limit and an attack threshold. The rate limit must be lower than the attack threshold. If the packet rate exceeds the rate limit on a port, the port discards the packets. If the packet rate exceeds the attack threshold on a port, the port logs the attacks and sends traps.

Related Configuration

Use ARP guard as an example:

Configuring the Global Port-based Rate Limit and Attack Threshold

In NFPP configuration mode:

Run the **arp-guard rate-limit per-port** *pps* command to configure the rate limit of a port.

Run the **arp-guard attack-threshold per-port** *pps* command to configure the attack threshold of a port.

Configuring Port-based Rate Limit and Attack Threshold on an Interface

In interface configuration mode:

Run the **nfpp arp-guard policy per-port** *rate-limit-pps attack-threshold-pps* command to configure the rate limit and attack threshold of a port.

15.3.3 Monitoring Period

Working Principle

The monitoring user provides information about attackers in the current system. If the isolation period is 0 (that is, not isolated), the guard module automatically performs software monitoring on attackers in the configured monitoring period. If the isolation period is set to a non-zero value, the guard module automatically isolates the hosts monitored by software.

During software monitoring, if the isolation period is set to a non-zero value, the guard module automatically isolates the attacker and sets the timeout period as the isolation period.

The monitoring period is valid only when the isolation period is 0.

Related Configuration

Use ARP guard as an example:

Configuring the Global Monitoring Period

In NFPP configuration mode:

Run the **arp-guard monitor-period** *seconds* command to configure the monitoring period.

15.3.4 Isolation Period

Working Principle

Isolation is performed by the guard policies after attacks are detected. Isolation is implemented using the filter of the hardware to ensure that these attacks will not be sent to the CPU, thereby ensuring proper running of the device.

Hardware isolation supports two modes: host-based and port-based isolation. At present, only ARP guard supports port-based hardware isolation.

A policy is configured in the hardware to isolate attackers. However, hardware resources are limited. When hardware resources are used up, the system prints logs to notify the administrator.

Related Configuration

Use ARP guard as an example:

Configuring the Global Isolation Period

In NFPP configuration mode:

Run the **arp-guard isolate-period** [*seconds* | **permanent**] command to configure the isolation period. If the isolation period is set to 0, isolation is disabled. If it is set to a non-zero value, the value indicates the isolation period. If it is set to **permanent**, ARP attacks are permanently isolated.

Configuring the Isolation Period on an Interface

In interface configuration mode:

Run the **nfpp arp-guard isolate-period** [*seconds* | **permanent**] command to configure the isolation period. If the isolation period is set to 0, isolation is disabled. If it is set to a non-zero value, the value indicates the isolation period. If it is set to **permanent**, ARP attacks are permanently isolated.

Enabling Isolate Forwarding

In NFPP configuration mode:

Run the **arp-guard isolate-forwarding enable** command to enable isolate forwarding.

Enabling Port-based Ratelimit Forwarding

In NFPP configuration mode:

Run the **arp-guard ratelimit-forwarding enable** command to enable port-based ratelimit forwarding.

At present, only ARP guard supports the configuration of isolate forwarding and ratelimit forwarding.

15.3.5 Trusted Hosts

Working Principle

If you do not want to monitor a host, you can run related commands to trust the host. This trusted host will be allowed to send packets to the CPU.

Related Configuration

Use IP anti-scanning as an example:

Configuring Trusted Hosts

In NFPP configuration mode:

Run the **ip-guard trusted-host** *ip mask* command to trust a host.

Run the **trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*} command to trust a host for a self-defined guard.

15.3.6 Centralized Bandwidth Allocation

Working Principle

Services defined in CPP are classified into three types: Manage, Route, and Protocol. (For details, see the following table.) Each type of service has an independent bandwidth. Different types of services cannot share their bandwidths. Traffics exceeding the bandwidth thresholds are discarded. By such service classification, service packets are processed by orders of precedence.

NFPP allows the administrator to flexibly assign bandwidth for three types of packets based on the actual network environment so that Protocol and Manage packets can be first processed. Prior processing of Protocol packets ensures proper running of protocols, and prior processing of Manage packets ensures proper management for the administrator, thereby ensuring proper running of important device functions and improving the guard capability of the device.

After classified rate limiting, all types of packets are centralized in a queue. When one type of service is processed inefficiently, packets of this service will be backlogged in the queue and may finally use up resources of the queue. NFPP allows the administrator to configure the percentages of these three types of packets in the queue. When the queue length occupied by one type of packets exceeds the value of the total queue length multiplied by the percentage of this packet type, the excessive packets will be discarded. This efficiently prevents one type of packets from exclusively occupying queue resources.

Packet Type	Service Type Defined in CPP
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, dhcps, gvrp, ripng, dvmrp, igmp, ospf, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c, option82
Route	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, non-ip-packet-other, arp
Manage	ip4-packet-local, ip6-packet-local

For the definitions of service types, see the Configuring CPU Protection.

Related Configuration

Configuring the Maximum Bandwidth of Specified Packets

In global configuration mode:

Run the **cpu-protect sub-interface** { **manage** | **protocol**|**route**} **pps** *pps_value* command to configure the maximum bandwidth of specified packets.

Configuring the Maximum Percentage of Specified Packets in the Queue

In global configuration mode:

Run the **cpu-protect sub-interface** { **manage** | **protocol** | **route**} **percent** *percent_value* command to configure the maximum percentage of specified packets in the queue.

15.4 Configuration

Configuration	Description and Command	
Configuring ARP Guard	**arp-guard enable**	Enables ARP guard globally.
	arp-guard isolate-period	Configures the global ARP-guard isolation period.
	arp-guard isolate-forwarding enable	Enables ARP-guard isolate forwarding.
	arp-guard ratelimit-forwarding enable	Enables APR-guard ratelimit forwarding.
	arp-guard monitor-period	Configures the global ARP-guard monitoring period.
	arp-guard monitored-host-limit	Configures the maximum number of ARP-guard monitored hosts.
	arp-guard rate-limit	Configures the global ARP-guard rate limit.

Configuration	Description and Command	
	arp-guard attack-threshold	Configures the global ARP-guard attack threshold.
	arp-guard scan-threshold	Configures the global ARP-guard scanning threshold.
	nfpp arp-guard enable	Enables ARP guard on an interface.
	nfpp arp-guard policy	Configures the APR-guard rate limit and attack threshold on an interface.
	nfpp arp-guard scan-threshold	Configures the APR-guard scanning threshold on an interface.
	nfpp arp-guard isolate-period	Configures the APR-guard isolation period on an interface.
Configuring IP Guard	**ip-guard enable**	Enables IP guard globally.
	ip-guard isolate-period	Configures the global IP-guard isolation period.
	ip-guard monitor-period	Configures the global IP-guard monitoring period.
	ip-guard monitored-host-limit	Configures the maximum number of IP-guard monitored hosts.
	ip-guard rate-limit	Configures the global IP-guard rate limit.
	ip-guard attack-threshold	Configures the global IP-guard attack threshold.
	ip-guard scan-threshold	Configures the global IP-guard scanning threshold.
	ip-guard trusted-host	Configures IP-guard trusted hosts.
	nfpp ip-guard enable	Enables IP guard on an interface.
	nfpp ip-guard policy	Configures the IP-guard rate limit and attack threshold on an interface.
	nfpp ip-guard scan-threshold	Configures the IP-guard scanning threshold on an interface.
	nfpp ip-guard isolate-period	Configures the IP-guard isolation period on an interface.
Configuring ICMP Guard	**icmp-guard enable**	Enables ICMP guard globally.
	icmp-guard isolate-period	Configures the global ICMP-guard isolation period.
	icmp-guard monitor-period	Configures the global ICMP-guard monitoring period.
	icmp-guard monitored-host-limit	Configures the maximum number of ICMP-guard monitored hosts.
	icmp-guard rate-limit	Configures the global ICMP-guard rate limit.
	icmp-guard attack-threshold	Configures the global ICMP-guard attack threshold.
	icmp-guard trusted-host	Configures ICMP-guard trusted hosts.

Configuration	Description and Command	
	nfpp icmp-guard enable	Enables ICMP guard on an interface.
	nfpp icmp-guard policy	Configures the ICMP-guard rate limit and attack threshold on an interface.
	nfpp icmp-guard isolate-period	Configures the ICMP-guard isolation period on an interface.
Configuring DHCP Guard	**dhcp-guard enable**	Enables DHCP guard globally.
	dhcp-guard isolate-period	Configures the global DHCP-guard isolation period.
	dhcp-guard monitor-period	Configures the global DHCP-guard monitoring period.
	dhcp-guard monitored-host-limit	Configures the maximum number of DHCP-guard monitored hosts.
	dhcp-guard rate-limit	Configures the global DHCP-guard rate limit.
	dhcp-guard attack-threshold	Configures the global DHCP-guard attack threshold.
	nfpp dhcp-guard enable	Enables DHCP guard on an interface.
	nfpp dhcp-guard policy	Configures the DHCP-guard rate limit and attack threshold on an interface.
	nfpp dhcp-guard isolate-period	Configures the DHCP-guard isolation period on an interface.
Configuring DHCPv6 Guard	**dhcpv6-guard enable**	Enables DHCPv6 guard globally.
	dhcpv6-guard isolate-period	Configures the global DHCPv6-guard isolation period.
	dhcpv6-guard monitor-period	Configures the global DHCPv6-guard monitoring period.
	dhcpv6-guard monitored-host-limit	Configures the maximum number of DHCPv6-guard monitored hosts.
	dhcpv6-guard rate-limit	Configures the global DHCPv6-guard rate limit.
	dhcpv6-guard attack-threshold { **per-src-mac** | **per-port**} *pps*	Configures the global DHCPv6-guard attack threshold.
	nfpp dhcpv6-guard enable	Enables DHCPv6 guard on an interface.
	nfpp dhcpv6-guard policy	Configures the DHCPv6-guard rate limit and attack threshold on an interface.
	nfpp dhcpv6-guard isolate-period	Configures the DHCPv6-guard isolation period on an interface.
Configuring ND Guard	**nd-guard enable**	Enables ND guard globally.
	nd-guard ratelimit-forwarding enable	Enables ND-guard ratelimit forwarding.
	nd-guard rate-limit per-port	Configures the global ND-guard rate limit.
	nd-guard attack-threshold per-port	Configures the global ND-guard attack threshold.

Configuration	Description and Command	
	nfpp nd-guard enable	Enables ND guard on an interface.
	nfpp nd-guard policy per-port	Configures the ND-guard rate limit and attack threshold on an interface.
Configuring a Self-Defined Guard	**define**	Configures the name of a self-defined guard.
	match	Configures **match** fields of a self-defined guard.
	global-policy	Configures the global rate limit and attack threshold of a self-defined guard.
	isolate-period	Configures the global isolation period of a self-defined guard.
	monitor-period	Configures the global monitoring period of a self-defined guard.
	monitored-host-limit	Configures the maximum number of monitored hosts of a self-defined guard.
	trusted-host	Configures trusted hosts of a self-defined guard.
	define *name* **enable**	Enables a self-defined guard globally.
	nfpp define *name* **enable**	Enables a self-defined guard on an interface.
	nfpp define	Configures the rate limit and attack threshold of a self-defined guard on an interface.
Configuring NFPP Logging	**log-buffer entries**	Configures the log buffer size.
	log-buffer logs	Configures the log buffer rate.
	logging vlan	Configures VLAN-based logging filtering.
	logging interface	Configures interface-based logging filtering.
	logging enable	Enables log printing.

15.4.1 Configuring ARP Guard

Configuration Effect

- ARP attacks are identified based on hosts or ports. Host-based ARP attack identification supports two modes: identification based on the source IP address, VLAN ID, and port and identification based on the link-layer source MAC address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the ARP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ARP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based attack identification, the system also isolates the attack source.
- ARP guard can also detect ARP scanning attacks. ARP scanning attacks indicate that the link-layer source MAC address is fixed but the source IP address changes, or that the link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes. Due to the possibility of false positive, hosts possibly performing ARP scanning are not isolated and are provided for the administrator's reference only.
- Configure ARP-guard isolation to assign hardware-isolated entries against host attacks so that attack packets are neither sent to the CPU nor forwarded.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- ARP guard prevents only ARP DoS attacks to the switch, but not ARP spoofing or ARP attacks in the network.
- For trusted ports configured for Dynamic ARP Inspection (DAI), ARP guard does not take effect, preventing false positive of ARP traffic over the trusted ports. For details about DAI trusted ports, see the Configuring Dynamic ARP Inspection.

Configuration Steps

Enabling ARP Guard

- (Mandatory) ARP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If ARP guard is disabled, the system automatically clears monitored hosts, scanned hosts, and isolated entries on ports.

Configuring the ARP-Guard Isolation Period

- (Optional) ARP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Enabling ARP-Guard Isolate Forwarding

- (Optional) ARP-guard isolate forwarding is enabled by default.
- To make isolation valid only at the management plane instead of the forwarding plane, you can enable this function.
- This function can be enabled in NFPP configuration mode.

Enabling ARP-Guard Ratelimit Forwarding

- (Optional) This function is enabled by default.
- If the port-based isolation entry takes effect, you can enable this function to pass some of the packets while not discarding all of them.
- This function can be enabled in NFPP configuration mode.

Configuring the ARP-Guard Monitoring Period

- (Mandatory) The default ARP-guard monitoring period is 600 seconds.

- If the ARP-guard isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of ARP-Guard Monitored Hosts

- (Mandatory) The maximum number of ARP-guard monitored hosts is 20,000 by default.
- Set the maximum number of ARP-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of ARP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the ARP-Guard Attack Threshold

- Mandatory.
- To achieve the best ARP-guard effect, you are advised to configure the host-based rate limit and attack threshold based on the following order: Source IP address-based rate limit < Source IP address-based attack threshold <Source MAC address-based rate limit <Source MAC address-based attack threshold.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over source IP address-based rate limiting while the latter takes priority over port-based rate limiting.

Configuring the ARP-Guard Scanning Threshold

- Mandatory.
- The scanning threshold can be configured in NFPP configuration mode or interface configuration mode.
- The ARP scanning table stores only the latest 256 records. When the ARP scanning table is full, the latest record will overwrite the earliest record.

- ARP scanning attack may have occurred if ARP packets received within 10 seconds meet either of the following conditions:
  - The link-layer source MAC address is fixed but the source IP address changes.
  - The link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes, and the change times exceed the scanning threshold.

Verification

When a host in the network sends ARP attack packets to a switch configured with ARP guard, check whether these packets can be sent to the CPU.

- If the packets exceed the attack threshold or scanning threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling ARP Guard Globally

Command	**arp-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ARP-Guard Isolation Period

Command	**arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling ARP-Guard Isolate Forwarding

Command	**arp-guard isolate-forwarding enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling ARP-Guard Ratelimit Forwarding

Command	**arp-guard ratelimit-forwarding enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ARP-Guard Monitoring Period

Command	**arp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Maximum Number of ARP-Guard Monitored Hosts

Command	**arp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ARP-Guard Rate Limit

Command	**arp-guard rate-limit** {**per-src-ip** |**per-src-mac	per-port**} *pps*
Parameter Description	**per-src-ip**: Limits the rate of each source IP address. **per-src-mac**: Limits the rate of each source MAC address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ARP-Guard Attack Threshold

Command	**arp-guard attack-threshold** {**per-src-ip	per-src-mac	per-port**} *pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-src-mac**: Configures the attack threshold of each source MAC address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is packets per second (pps).
Command	NFPP configuration mode

Mode	
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Global ARP-Guard Scanning Threshold

Command	**arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling ARP Guard on an Interface

Command	**nfpp arp-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	ARP guard configured in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuring the ARP-Guard Isolation Period on an Interface

Command	**nfpp arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the ARP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp arp-guard policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-src-ip**: Configures the rate limit and attack threshold of each source MAC address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the ARP-Guard Scanning Threshold on an Interface

Command	**nfpp arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

CPU Protection Based on ARP Guard

Scenario	● ARP host attacks exist in the system, and some hosts fail to properly establish ARP connection. ● ARP scanning exists in the system, causing a very high CPU utilization rate.
Configuration Steps	● Set the host-based attack threshold to 5 pps. ● Set the ARP scanning threshold to 10 pps. ● Set the isolation period to 180 pps.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#arp-guard rate-limit per-src-mac 5 Hostname (config-nfpp)#arp-guard attack-threshold per-src-mac 10 Hostname (config-nfpp)#arp-guard isolate-period 180
Verification	● Run the **show nfpp arp-guard summary** command to display the configuration.
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold Global Disable 180 4/5/100 8/10/200 15 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp arp-guard hosts** command to display the monitored hosts.
	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.

```
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)
```

Common Errors

N/A

15.4.2 Configuring IP Guard

Configuration Effect

- IP attacks are identified based on hosts or physical interfaces. In host-based IP attack identification, IP attacks are identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the IP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the IP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based attack identification, the system also isolates the attack source.
- IP guard can also detect IP scanning attacks. IP anti-scanning applies to IP packet attacks as follows: the destination IP address continuously changes but the source IP address remains the same, and the destination IP address is not the IP address of the local device.
- Configure IP guard isolation to assign hardware-isolated entries against host attacks so that attack packets are neither sent to the CPU nor forwarded.
- IP anti-scanning applies to IP packet attacks where the destination IP address is not the local IP address. The CPP limits the rate of IP packets where the destination IP address is the local IP address.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.

Configuration Steps

↘ Enabling IP Guard

- (Mandatory) IP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.

- If IP guard is disabled, the system automatically clears monitored hosts.

Configuring the IP-Guard Isolation Period

- (Optional) IP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the IP-Guard Monitoring Period

- (Mandatory) The default IP-guard monitoring period is 600 seconds.
- If the IP-guard isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of IP-Guard Monitored Hosts

- (Mandatory) The maximum number of IP-guard monitored hosts is 20,000 by default.
- Set the maximum number of IP-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of IP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the IP-Guard Attack Threshold

- Mandatory.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.

Configuring the IP-Guard Scanning Threshold

- Mandatory.
- The scanning threshold can be configured in NFPP configuration mode or interface configuration mode.
- ARP scanning attack may have occurred if ARP packets received within 10 seconds meet the following conditions:
  - The source IP address remains the same.
  - The destination IP address continuously changes and is not the local IP address, and the change times exceed the scanning threshold.

Configuring IP-Guard Trusted Hosts

- (Optional) No IP-guard trusted host is configured by default.
- For IP guard, you can only configure a maximum of 500 IP addresses not to be monitored.
- Trusted hosts can be configured in NFPP configuration mode.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If a host cannot be trusted, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the host to trust already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the host to delete from the trusted table does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.
- If the memory cannot be allocated to a trusted host, the system prints the log "%ERROR: Failed to alloc memory." to notify the administrator.

Verification

When a host in the network sends IP attack packets to a switch configured with IP guard, check whether these packets can be sent to the CPU.

- If the rate of packets from untrusted hosts exceeds the attack threshold or scanning threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling IP Guard Globally

Command	**ip-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Isolation Period

Command	**ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Monitoring Period

Command	**ip-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of IP-Guard Monitored Hosts

Command	**ip-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global IP-Guard Rate Limit

Command	**ip-guard rate-limit** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Limits the rate of each source IP address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode

Usage Guide	N/A

Configuring the Global IP-Guard Attack Threshold

Command	**ip-guard attack-threshold** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Global IP-Guard Scanning Threshold

Command	**ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring IP-Guard Trusted Hosts

Command	**ip-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address. **all**: Used with **no** to delete all trusted hosts.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run this command to trust the host. This trusted host can send IP packets to the CPU, without any rate limiting or alarm reporting.

Enabling IP Guard on an Interface

Command	**nfpp ip-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IP guard configured in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuring the IP-Guard Isolation Period on an Interface

Command	**nfpp ip-guard isolate-period** [*seconds* | **permanent**]

Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the IP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp ip-guard policy** {**per-src-ip**| **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-port**: Configures the attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the IP-Guard Scanning Threshold on an Interface

Command	**nfpp ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

CPU Protection Based on IP Guard

Scenario	● IP host attacks exist in the system, and packets of some hosts cannot be properly routed and forwarded. ● IP scanning exists in the system, causing a very high CPU utilization rate. ● Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Configure the IP scanning threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.

	`Hostname# configure terminal`
	`Hostname(config)# nfpp`
	`Hostname (config-nfpp)#ip-guard rate-limit per-src-ip 20`
	`Hostname (config-nfpp)#ip-guard attack-threshold per-src-ip 30`

	Hostname (config-nfpp)#ip-guard isolate-period 180 Hostname (config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255
Verification	● Run the **show nfpp ip-guard summary** command to display the configuration.
	(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.
	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.
	IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

Common Errors

N/A

15.4.3 Configuring ICMP Guard

Configuration Effect

- ICMP attacks are identified based on hosts or ports. In host-based attack identification, ICMP attacks are identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the ICMP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ICMP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based attack identification, the system also isolates the attack source.
- Configure ICMP guard isolation to assign hardware-isolated entries against host attacks so that attack packets are neither sent to the CPU nor forwarded.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.

Configuration Steps

Enabling ICMP Guard

- (Mandatory) ICMP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If ICMP guard is disabled, the system automatically clears monitored hosts.

Configuring the ICMP-Guard Isolation Period

- (Optional) ICMP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the ICMP-Guard Monitoring Period

- (Mandatory) The default ICMP-guard monitoring period is 600 seconds.
- If the ICMP-guard isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of ICMP-Guard Monitored Hosts

- (Mandatory) The maximum number of ICMP-guard monitored hosts is 20,000 by default.
- Set the maximum number of ICMP-guard monitored hosts reasonably. As the number of actually monitored hosts increases, more CPU resources are used.
- The maximum number of ICMP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the ICMP-Guard Attack Threshold

- Mandatory.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ICMP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.

Configuring ICMP-Guard Trusted Hosts

- (Optional) No ICMP-guard trusted host is configured by default.
- For ICMP guard, you can only configure a maximum of 500 IP addresses not to be monitored.
- Trusted hosts can be configured in NFPP configuration mode.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If a host cannot be trusted, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the host to trust already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the host to delete from the trusted table does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.
- If the memory cannot be allocated to a trusted host, the system prints the log "%ERROR: Failed to alloc memory." to notify the administrator.

Verification

When a host in the network sends ICMP attack packets to a switch configured with ICMP guard, check whether these packets can be sent to the CPU.

- If the rate of packets from an untrusted host exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling ICMP Guard Globally

Command	**icmp-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ICMP-Guard Isolation Period

Command	**icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Configuring the Global ICMP-Guard Monitoring Period

Command	**icmp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs hardware isolation against monitored attackers and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of ICMP-Guard Monitored Hosts

Command	**icmp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The

	value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the Global ICMP-Guard Rate Limit

Command	**icmp-guard rate-limit** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Limits the rate of each source IP address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ICMP-Guard Attack Threshold

Command	**icmp-guard attack-threshold** {**per-src-ip** | **per-port**} *pps*
Parameter Description	**per-src-ip**: Configures the attack threshold of each source IP address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring ICMP-Guard Trusted Hosts

Command	**icmp-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address. **all**: Used with **no** to delete all trusted hosts.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run this command to trust the host. This trusted host can send ICMP packets to the CPU, without any rate limiting or alarm reporting. You can configure the mask so that no host in one network segment is monitored. You can configure a maximum of 500 trusted hosts.

Enabling ICMP Guard on an Interface

Command	**nfpp icmp-guard enable**
Parameter Description	N/A
Command	Interface configuration mode

Mode	
Usage Guide	ICMP guard configured in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuring the ICMP-Guard Isolation Period on an Interface

Command	**nfpp icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the ICMP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp icmp-guard policy** {**per-src-ip** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on ICMP Guard

Scenario	● ICMP host attacks exist in the system, and some hosts cannot successfully ping devices. ● Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.

	`Hostname# configure terminal`
	`Hostname(config)# nfpp`
	`Hostname (config-nfpp)#icmp-guard rate-limit per-src-ip 20`
	`Hostname (config-nfpp)#icmp-guard attack-threshold per-src-ip 30`
	`Hostname (config-nfpp)#icmp-guard isolate-period 180`
	`Hostname (config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255`

Verification	● Run the **show nfpp icmp-guard summary** command to display the configuration.

	(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 Global Disable 180 20/-/400 30/-/400 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp icmp-guard hosts** command to display the monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address remain-time(s) ---- --------- ---------- -------------- 1 Gi0/5 192.168.201.47 160 Total: 1 host
	● Run the **show nfpp icmp-guard trusted-host** command to display the trusted hosts.
	IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

Common Errors

N/A

15.4.4 Configuring DHCP Guard

Configuration Effect

- DHCP attacks are identified based on hosts or ports. In host-based attack identification, DHCP attacks are identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the DHCP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCP packet rate exceeds the attack threshold, the system prints alarm information and sends traps. In host-based attack identification, the system also isolates the attack source.
- Configure DHCP guard isolation to assign hardware-isolated entries against host attacks so that attack packets are neither sent to the CPU nor forwarded.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.

- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- For trusted ports configured for DHCP snooping, DHCP guard does not take effect, preventing false positive of DHCP traffic on the trusted ports. For details about trusted ports of DHCP snooping, see "Configuring Basic Functions of DHCP Snooping" in the Configuring DHCP Snooping.

Configuration Steps

Enabling DHCP Guard

- (Mandatory) DHCP guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.
- If DHCP guard is disabled, the system automatically clears monitored hosts.

Configuring the DHCP-Guard Isolation Period

- (Optional) DHCP-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the DHCP-Guard Monitoring Period

- (Mandatory) DHCP-guard monitoring is enabled by default.
- If the DHCP-guard isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of DHCP-Guard Monitored Hosts

- (Mandatory) The maximum number of DHCP-guard monitored hosts is 20,000 by default.
- Set the maximum number of DHCP-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of DHCP-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the DHCP-Guard Attack Threshold

- Mandatory.
- The attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.

Verification

When a host in the network sends DHCP attack packets to a switch configured with DHCP guard, check whether these packets can be sent to the CPU.

- If the parameter of the packets exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling DHCP Guard Globally

Command	**dhcp-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCP-Guard Isolation Period

Command	**dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Configuring the Global DHCP-Guard Monitoring Period

Command	**dhcp-guard monitor-period** *seconds*

Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs hardware isolation against monitored attackers and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of DHCP-Guard Monitored Hosts

Command	**dhcp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the Global DHCP-Guard Rate Limit

Command	**dhcp-guard rate-limit** {**per-src-mac**	**per-port**} *pps*
Parameter Description	**per-src-mac**: Limits the rate of each source MAC address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCP-Guard Attack Threshold

Command	**dhcp-guard attack-threshold** {**per-src-mac**	**per-port**} *pps*
Parameter Description	**per-src-mac**: Configures the attack threshold of each source MAC address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command	NFPP configuration mode

Mode	
Usage Guide	N/A

Enabling DHCP Guard on an Interface

Command	**nfpp dhcp-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	DHCP guard configured in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuring the DHCP-Guard Isolation Period on an Interface

Command	**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the DHCP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp dhcp-guard policy** {**per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on DHCP Guard

Scenario	● DHCP host attacks exist in the system, and some hosts fail to request IP addresses.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#dhcp-guard rate-limit per-src-mac 8

	Hostname (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16 Hostname (config-nfpp)#dhcp-guard isolate-period 180
Verification	● Run the **show nfpp dhcp-guard summary** command to display the configuration.
	(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 Global Disable 180 -/8/150 -/16/300 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp dhcp-guard hosts** command to display the monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ---------- --------------- *1 Gi0/5 001a.a9c2.4609 160 Total: 1 host

Common Errors

N/A

15.4.5 Configuring DHCPv6 Guard

Configuration Effect

- DHCPv6 attacks are identified based on hosts or ports. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an attack threshold. If the DHCPv6 packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCPv6 packet rate exceeds the attack threshold, the system prints alarm information and sends traps.
- In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- For trusted ports configured for DHCPv6 snooping, DHCPv6 guard does not take effect, preventing false positive of DHCPv6 traffic on the trusted ports. For details about trusted ports of DHCPv6 snooping, see "Configuring Basic Functions of DHCPv6 Snooping" in the Configuring DHCPv6 Snooping.

Configuration Steps

Enabling DHCPv6 Guard

- (Mandatory) DHCPv6 guard is enabled by default.
- DHCPv6 guard can be enabled in NFPP configuration mode or interface configuration mode.
- If DHCPv6 guard is disabled, the system automatically clears monitored hosts.

Configuring the DHCPv6-Guard Isolation Period

- (Optional) DHCPv6-guard isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The DHCPv6-guard isolation period can be configured in NFPP configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the DHCPv6-Guard Monitoring Period

- (Mandatory) The default DHCPv6-guard monitoring period is 600 seconds.
- If the DHCPv6-guard isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period does not take effect.
- The DHCPv6-guard monitoring period can be configured in NFPP configuration mode.

Configuring the Maximum Number of DHCPv6-Guard Monitored Hosts

- (Mandatory) The maximum number of DHCPv6-guard monitored hosts is 20,000 by default.
- Set the maximum number of DHCPv6-guard monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of DHCPv6-guard monitored hosts can be configured in NFPP configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the DHCPv6-Guard Attack Threshold

- Mandatory.
- The DHCPv6-guard attack threshold can be configured in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.

- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.

Verification

When a host in the network sends DHCPv6 attack packets to a switch configured with DHCPv6 guard, check whether these packets can be sent to the CPU.

- If the parameter of the packets exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Enabling DHCPv6 Guard Globally

Command	**dhcpv6-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCPv6-Guard Isolation Period

Command	**dhcpv6-guardisolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Configuring the Global DHCPv6-Guard Monitoring Period

Command	**dhcpv6-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout

	period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs hardware isolation against monitored attackers and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of DHCPv6-Guard Monitored Hosts

Command	**dhcpv6-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts." to notify the administrator.

Configuring the Global DHCPv6-Guard Rate Limit

Command	**dhcpv6-guardrate-limit** { **per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-mac**: Limits the rate of each source MAC address. **per-port**: Limits the rate of each port. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global DHCPv6-Guard Attack Threshold

Command	**dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port**} *pps*
Parameter Description	**per-src-mac**: Configures the attack threshold of each source MAC address. **per-port**: Configures the attack threshold of each port. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling DHCPv6 Guard on an Interface

Command	**nfpp dhcpv6-guard enable**

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	DHCPv6 guard configured in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuring the DHCPv6-Guard Isolation Period on an Interface

Command	**nfpp dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the DHCP-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp dhcpv6-guard policy** {**per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on DHCPv6 Guard

Scenario	● DHCPv6 host attacks exist in the system, and DHCPv6 neighbor discovery fails on some hosts.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8 Hostname (config-nfpp)#dhcpv6-guard attack-threshold per-src-mac 16 Hostname (config-nfpp)#dhcpv6-guard isolate-period 180
Verification	● Run the **show nfpp dhcpv6-guard summary** command to display the configuration.
	(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 Global Disable 180 -/8/150 -/16/300 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp dhcpv6-guard hosts** command to display the monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 001a.a9c2.4609 160 Total: 1 host

Common Errors

N/A

15.4.6 Configuring ND Guard

Configuration Effect

- AR ND guard classifies ND packets into three types based on their purposes: 1. NS and NA; 2. RS; 3. RA and Redirect. Type 1 packets are used for address resolution. Type 2 packets are used by hosts to discover the gateway. Type 3 packets are related to routing: RAs are used to advertise the gateway and prefix while Redirect packets are used to advertise a better next hop.
- At present, only port-based ND packet attack identification is supported. You can configure the rate limits and attack thresholds for these three types of packets respectively. If the ND packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ND packet rate exceeds the attack threshold, the system prints logs and sends traps.

Notes

- For a command that is configured both in NFPP configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in NFPP configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.

Configuration Steps

↘ Enabling ND Guard

- (Mandatory) ND guard is enabled by default.
- This function can be enabled in NFPP configuration mode or interface configuration mode.

Enabling ND-Guard Ratelimit Forwarding

- (Optional) This function is enabled by default.
- If the port-based isolation entry takes effect, you can enable this function to pass some of the packets while not discarding all of them.
- This function can be enabled in NFPP configuration mode.

Configuring the ND-Guard Attack Threshold

- Mandatory.
- The ND-guard attack threshold can be enabled in NFPP configuration mode or interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If memories cannot assigned to detected attackers, the system prints the log "%NFPP_ND_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.

Verification

When a host in the network sends ND attack packets to a switch configured with ND guard, check whether these packets can be sent to the CPU.

- If the parameter of the packets exceeds the attack threshold, an attack log is displayed.

Related Commands

Enabling ND Guard Globally

Command	**nd-guard enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Enabling ND-Guard Ratelimit Forwarding

Command	**nd-guard ratelimit-forwarding enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ND-Guard Rate Limit

Command	**nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *pps*: Indicates the rate limit, ranging from 1 to 19,999.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Global ND-Guard Attack Threshold

Command	**nd-guard attack-threshold per-port**[**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *pps*: Indicates the attack threshold, ranging from 1 to 19,999. The unit is pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Enabling ND Guard on an Interface

Command	**nfpp nd-guard enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	ND guard configured in interface configuration mode takes priority over that configured in NFPP configuration mode.

Configuring the ND-Guard Rate Limit and Attack Threshold on an Interface

Command	**nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

CPU Protection Based on ND Guard

Scenario	● ND host attacks exist in the system, and neighbor discovery fails on some hosts.
Configuration Steps	● Configure the host-based attack threshold.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)# nd-guard rate-limit per-port ns-na 30 Hostname (config-nfpp)# nd-guard attack-threshold per-port ns-na 50
Verification	● Run the **show nfpp nd-guard summary** command to display the configuration.
	(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.) Interface Status Rate-limit Attack-threshold Global Disable 30/15/15

Common Errors

N/A

15.4.7 Configuring a Self-Defined Guard

Configuration Effect

- Configure a self-defined guard to resolve network attack problems in special scenarios.

Notes

- For a command that is configured both in self-defined guard configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in self-defined guard configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy hardware entries of the security module.
- A self-defined guard takes priority over basic guards. When configuring the match fields of self-defined guards, see the Configuration Guide.

Configuration Steps

Configuring the Guard Name

- (Mandatory) Configure the name of a self-defined guard to create the self-defined guard.
- The guard name must be unique, and the match fields and values c must be different from those of ARP, ICMP, DHCP, IP, and DHCPv6 guards. If the parameters you want to configure already exist, a message is displayed to indicate the configuration failure.

Configuring the Match Fields

- Mandatory.
- Self-defined packets are classified based on the following fields: etype (Ethernet link-layer type), smac (source MAC address), dmac (destination MAC address), protocol (IPv4/IPv6 protocol number), sip (source IPv4/IPv6 address), dip (destination IPv4/IPv6 address), sport (source transport-layer port), and dport (destination transport-layer port).
- **protocol** is valid only when the value of **etype** is **ipv4** or **ipv6**. **src-ip** and **dst-ip** are valid only when the value of **etype** is **ipv4**. **src-ipv6** and **dst-ipv6** are valid only when the value of **etype** is **ipv6**. **src-port** and **dst-port** are valid only when the value of **protocol** is **tcp** or **udp**.
- If the **match** fields and values of a self-defined guard are totally the same as those of an existing guard, the system prints the log "%ERROR: the match type and value are the same with define name (name of an existing guard)." to notify the administrator of the configuration failure.
- If **protocol** is configured but **etype** is IPv4 or IPv6 in the **match** policy, the system prints the log "%ERROR: protocol is valid only when etype is IPv4(0x0800) or IPv6(0x86dd)."
- If **src-ip** and **dst-ip** are configured but **etype** is not IPv4 in the **match** policy, the system prints the log "%ERROR: IP address is valid only when etype is IPv4(0x0800)."
- If **src-ipv6** and **dst-ipv6** are configured but **etype** is not IPv6 in the **match** policy, the system prints the log "%ERROR: IPv6 address is valid only when etype is IPv6(0x86dd)."
- If **src-port** and **dst-port** are configured but **protocol** is not TCP or UDP in the **match** policy, the system prints the log "%ERROR: Port is valid only when protocol is TCP(6) or UDP(17)."
- The following table lists guard policies corresponding to some common network protocols. The rate limits and attack thresholds listed below can meet the requirements in most network scenarios and are for reference only. You can configure valid rate limits and attack thresholds based on actual scenarios.

Protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
RIP	etype 0x0800 protocol 17 dst-port 520	rate-limit 100 attatch-threshold 150	Not applicable to this policy	rate-limit 300 attatch-threshold 500
RIPng	etype 0x86dd protocol 17 dst-port 521	rate-limit 100 attatch-threshold 150	Not applicable to this policy	rate-limit 300 attatch-threshold 500
BPDU	dst-mac 0180.c200.0000	Not applicable to this policy	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
RERP	dst-mac 01d0.f800.0001	Not applicable to this policy	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
REUP	dst-mac 01d0.f800.0007	Not applicable to this policy	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
OSPFv2	etype 0x0800 protocol 89	rate-limit 800 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000
OSPFv3	etype 0x86dd protocol 89	rate-limit 800 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000

Protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
VRRP	etype 0x0800 protocol 112	rate-limit 64 attatch-threshold 100	Not applicable to this policy	rate-limit 1024 attatch-threshold 1024
IPv6 VRRP	etype 0x86dd protocol 112	rate-limit 64 attatch-threshold 100	Not applicable to this policy	rate-limit 1024 attatch-threshold 1024
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attatch-threshold 1200	Not applicable to this policy	rate-limit 2000 attatch-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attatch-threshold 1200	Not applicable to this policy	rate-limit 1200 attatch-threshold 1500
LDP (UDP hello)	etype 0x0800 protocol 17 dst-port 646	rate-limit 10 attatch-threshold 15	Not applicable to this policy	rate-limit 100 attatch-threshold 150

- To contain as many existing protocol types as possible and facilitate expansion of new protocol types, self-defined guards allow hosts to freely combine type fields of packets. If the configuration is inappropriate, the network may become abnormal. Therefore, the network administrator needs to have a good knowledge of network protocols. As a reference, the following table lists valid configurations of currently known protocols for common self-defined guard policies. For other protocols not listed in the table, configure them with caution.

Configuring the Global Rate Limit and Attack Threshold

- (Mandatory) If these parameters are not configured, the self-defined guard cannot be enabled.
- You must configure one of the per-src-ip, per-src-mac, and per-port fields. Otherwise, the policy cannot take effect.
- per-src-ip is valid only when etype is IPv4 or IPv6.
- The rate limit configured based on the source MAC address, VLAN ID, and port takes priority over that configured based on the source IP address, VLAN ID, and port.
- The port-based host identification policy of a self-defined guard must be consistent with the global port-based host identification policy.
- If the **per-src-ip** policy is not configured globally but configured for a port, the system prints the log "%ERROR: name (name of a self-defined guard) has not per-src-ip policy." to notify the administrator of the configuration failure.
- If the **per-src-mac** policy is not configured globally but configured for a port, the system prints the log "%ERROR: name (name of a self-defined guard) has not per-src-mac policy." to notify the administrator of the configuration failure.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DEFINE_GUARD-4-NO_MEMORY: Failed to allocate memory." to notify the administrator.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is less than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.

Configuring the Global Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit defined in CPP, you can configure the isolation period to discard packets and therefore to save bandwidth resources.
- The isolation period can be configured in self-defined guard configuration mode or interface configuration mode.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Global Monitoring Period

- (Mandatory) The default monitoring period is 600 seconds.
- If the isolation period is configured, it is directly used as the monitoring period, and the configured monitoring period will lose effect.
- The monitoring period can be configured in self-defined guard configuration mode.
- If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs hardware isolation against monitored attackers and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored.

Configuring the Maximum Number of Monitored Hosts

- (Mandatory) The maximum number of monitored hosts is 20,000 by default.
- Set the maximum number of monitored hosts reasonably. As the number of monitored hosts increases, more CPU resources are used.
- The maximum number of monitored hosts can be configured in self-defined guard configuration mode.
- If the number of monitored hosts reaches 20,000 (default value) and the administrator sets the maximum number lower than 20,000, the system does not delete monitored hosts but prints the log "%ERROR: The value that you configured is smaller than current monitored hosts 20000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 20000 monitored hosts." to notify the administrator.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- You can configure a maximum of 500 trusted IP address or MAC address for a self-defined guard.
- Trusted hosts can be configured in self-defined guard configuration mode.
- If you do not want to monitor a host, you can run the following commands to trust the host. This trusted host can send ICMP packets to the CPU, without any rate limiting or alarm reporting. You can configure the mask so that no host in one network segment is monitored.

- You must configure the **match** type before configuring trusted hosts. If the packet type is IPv4 in the **match** policy, you are not allowed to configure trusted IPv6 addresses. If the packet type is IPv6 in the match policy, you are not allowed to configure trusted IPv4 addresses.
- If the **match** type is not configured, the system prints the log "%ERROR: Please configure match rule first."
- If a trusted IPv4 host is added but **etype** is not IPv4 in the **match** policy, the system prints the log "%ERROR: Match type can't support IPv4 trusted host."
- If a trusted IPv6 host is added but **etype** is not IPv6 in the **match** policy, the system prints the log "%ERROR: Match type can't support IPv6 trusted host."
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If a trusted host cannot be deleted, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If a host cannot be trusted, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the host to trust already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the host to delete from the trusted table does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.
- If the memory cannot be allocated to a trusted host, the system prints the log "%ERROR: Failed to allocate memory." to notify the administrator.

Enabling a Self-Defined Guard

- Mandatory.
- You have to configure at least one policy between host-based self-defined guard policy and port-based self-defined guard policy. Otherwise, the self-defined guard cannot be enabled.
- If a self-defined guard is disabled, the system automatically clears monitored hosts.
- Self-defined guards can be configured in self-defined guard configuration mode or interface configuration mode.
- If a self-defined guard policy is not completely configured, the self-defined guard cannot be enabled and a prompt is displayed to notify hosts of the missing policy configurations.
- If the name of a self-defined guard does not exist, the system prints the log "%ERROR: The name is not exist."
- If the match type is not configured for a self-defined guard, the system prints the log "%ERROR: name (name of the self-defined guard) doesn't match any type."
- If no policy is configured for a self-defined guard, the system prints the log "%ERROR: name (name of the self-defined guard) doesn't specify any policy."

Verification

When a host in the network sends packets to a switch configured with a self-defined NFPP guard, check whether these packets can be sent to the CPU.

- If the rate of packets from an untrusted host exceeds the attack threshold, an attack log is displayed.
- If an isolated entry is created for the attacker, an isolation log is displayed.

Related Commands

Configuring the Name of a Self-defined Guard

Command	**define** *name*
Parameter Description	**name**: Indicates the name of a self-defined guard.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring Match Fields of a Self-defined Guard

Command	**match** [**etype***type*] [**src-mac***smac* [**src-mac-mask***smac_mask*]] [**dst-mac***dmac* [**dst-mac-mask***dst_mask*]] [**protocol***protocol*] [**src-ip***sip* [**src-ip-mask***sip-mask*]] [**src-ipv6***sipv6* [**src-ipv6-masklen***sipv6-masklen*]] [**dst-ip***dip***[dst-ip-mask***dip-mask*]] **[dst-ipv6***dipv6* [**dst-ipv6-masklen***dipv6-masklen*]][**src-port***sport*] [**dst-port** *dport*]
Parameter Description	*type*: Indicates the type of Ethernet link-layer packets. *smac*: Indicates the source MAC address. *smac_mask*: Indicates the mask of the source MAC address. *dmac*: Indicates the destination MAC address. *dst_mask*: Indicates the mask of the destination MAC address. *protocol*: Indicates the protocol number of IPv4/IPv6 packets. *sip*: Indicates the source IPv4 address. *sip-mask*: Indicates the mask of the source IPv4 address. *sipv6*: Indicates the source IPv6 address. *sipv6-masklen*: Indicates the mask length of the source IPv6 address. *dip*: Indicates the destination IPv4 address. *dip-mask*: Indicates the mask of the destination IPv4 address. *dipv6*: Indicates the destination IPv6 address. *dipv6-masklen*: Indicates the mask length of the destination IPv6 address. *sport*: Indicates the ID of the source transport-layer port. *dsport*: Indicates the ID of the destination transport-layer port.
Command Mode	Self-defined guard configuration mode
Usage Guide	Create a new self-defined guard and specify the packet fields matched by this guard.

Configuring the Global Rate Limit and Attack Threshold of a Self-defined Guard

Command	**global-policy** {**per-src-ip** | **per-src-mac** | **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip**: Collects rate statistics for host identification based on the source IP address, VLAN ID, and port. **per-src-mac**: Collects rate statistics for host identification based on the source MAC address, VLAN ID, and port. **per-port**: Collects rate statistics based on each packet receiving port. *rate-limit-pps*: Indicates the rate limit. *attack-threshold-pps*: Indicates the attack threshold.
Command Mode	Self-defined guard configuration mode
Usage Guide	Before creating a self-defined guard type, you must specify rate statistic classification rules for this type, namely, source IP address-based host identification, source MAC address-based host identification, host-based self-defined packet rate statistics, or port-based rate statistics, and specify the rate limits and attack thresholds for the specified rules.

Configuring the Global Isolation Period of a Self-defined Guard

Command	**isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Command Mode	Self-defined guard configuration mode
Usage Guide	If the isolation period is not 0, a host is isolated and its packets of the self-defined guard type are discarded when the packet rate of the self-defined guard exceeds the attack threshold.

Configuring the Global Monitoring Period of a Self-defined Guard

Command	**monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Monitored Hosts of a Self-defined Guard

Command	**monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Configuring Trusted Hosts of a Self-defined Guard

Command	**trusted-host** {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}
Parameter Description	*mac*: Indicates the MAC address. *mac_mask*: Indicates the mask of an MAC address. *ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address. *IPv6/prefixlen*: Indicates the IPv6 address and its mask length. **all**: Used with **no** to delete all trusted hosts.
Command Mode	Self-defined guard configuration mode
Usage Guide	N/A

Enabling a Self-Defined Guard Globally

Command	**define** *name* **enable**
Parameter Description	*name*: Indicates the name of a self-defined guard.
Command Mode	NFPP configuration mode
Usage Guide	The configuration takes effect only after you have configured **match**, **rate-count**, **rate-limit**, and **attack-threshold**. Otherwise, the configuration fails.

Enabling a Self-defined Guard on an Interface

Command	**nfpp define** *name* **enable**
Parameter Description	*name*: Indicates the name of a self-defined guard.
Command Mode	Interface configuration mode
Usage Guide	The self-defined name must exist. The configuration takes effect only after you have configured **match**, **rate-count**, **rate-limit**, and **attack-threshold**. Otherwise, the configuration fails.

Configuring the Rate Limit and Attack Threshold of a Self-defined Guard on an Interface

Command	**nfpp define** *name* **policy** {**per-src-ip** | **per-src-mac**| **per-port**} *rate-limit-pps attack-threshold-pps*
Parameter Description	*name*: Indicates the name of a self-defined guard. **per-src-ip**: Configures the rate limit and attack threshold of each source IP address. **per-src-mac**: Configures the rate limit and attack threshold of each source MAC address. **per-port**: Configures the rate limit and attack threshold of each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 19,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 19,999.
Command Mode	Interface configuration mode

Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuration Example

↘ CPU Protection Based on a Self-Defined Guard

Scenario	● Basic guards cannot protect the system with RIP attacks.
Configuration Steps	● Configure a self-defined guard, with the key fields matching RIP packets. ● Configure the rate limit. ● Configure the isolation period. ● Configure trusted hosts.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#define rip Hostname (config-nfpp-define)#match etype 0x0800 protocol 17 dst-port 520 Hostname (config-nfpp-define)#global-policy per-src-ip 100 150 Hostname (config-nfpp-define)# isolate-period 180 Hostname (config-nfpp-define)#trusted-host 192.168.201.46 255.255.255.255 Hostname (config-nfpp-define)#exit Hostname (config-nfpp)#define rip enable
Verification	● Run the **show nfpp define summary rip** command to display the configuration.
	Define rip summary: match etype 0x800 protocol 17 dst-port 520 Maximum count of monitored hosts: 1000 Monitor period:600s (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 Global Enable 180 100/-/- 150/-/-
	● Run the **show nfpp define trusted-host rip** command to display the trusted hosts.
	Define rip: IP trusted host number is 1: IP address IP mask ---------- ------- 192.168.201.46 255.255.255.255

	Total: 1 record(s)Global Enable 180 100/-/- 150/-/-
	● Run the **show nfpp define hosts rip** command to display the monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address remain-time(s) ---- --------- ---------- -------------- 1 Gi0/5 192.168.201.47 160 Total: 1 host

Common Errors

N/A

15.4.8 Configuring Centralized Bandwidth Allocation

Configuration Effect

- Configure centralized bandwidth allocation so that Manage and Protocol packets are first processed when the network is busy.

Notes

- The following condition must be met: Valid percentage range of a type of packets ≤ 100% – Percentage of the sum of the other two types

Configuration Steps

↘ Configuring the Maximum Bandwidth of Specified Packets

- (Mandatory) Manage, Route, and Protocol packets share the same default bandwidth.

↘ Configuring the Maximum Percentage of Specified Packets in the Queue

- (Mandatory) By default, Manage packets occupy 30% of the bandwidth, Route packets occupy 25%, and Protocol packets occupy 45%.

Verification

Send a large number of protocol packets such as OSPF packets to a switch, causing high CPU utilization.

- When the host pings the switch, the pinging must be successful and no packet is lost.

Related Commands

↘ Configuring the Maximum Bandwidth of Specified Packets

Command	**cpu-protect sub-interface** { **manage** | **protocol**|**route**} **pps** *pps_value*

Parameter Description	*pps_value*: Indicates the rate limit, ranging from 1 to 100,000.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Percentage of Specified Packets in the Queue

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route**} **percent** *percent_value*
Parameter Description	*percent_value*: Indicates the percentage of a type of packets in the queue, ranging from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	The following condition must be met: Valid percentage range of a type of packets ≤ 100% – Percentage of the sum of the other two types

Configuration Example

Prioritizing Packets Sent to the CPU Through Centralized Bandwidth Allocation

Scenario	● Various types of mass packets exist in the network and belong to different centralized types.
Configuration Steps	● Configure the maximum bandwidth of specified packets. ● Configure the maximum percentage of specified packets in the queue.

	`Hostname# configure terminal`
	`Hostname(config)# cpu-protect sub-interface manage pps 5000`
	`Hostname(config)# cpu-protect sub-interface manage percent 25`

Verification	N/A

Common Errors

N/A

15.4.9 Enabling/Disabling All Guards

Configuration Effect

- Use the (no) all-guard enable command to enable or disable all attack guards so that you do not need to disable or enable them one by one.

Notes

- Only basic guards (ARP, ICMP, IP, DHCP, DHCPv6, and ND) are applied.
- Only the global configuration is applied. Interface-based guard configuration remains the same.
- After the command is executed, basic guards are displayed by using the **show running-config** command.

- The **no all-guard enable** command just packs the **no** commands of all basic guards together. After you run the disabling command, the **no** commands of all basic guards are displayed under the **show running-config** command. After you run the enabling command, the default conditions are displayed under the **show running-config** command.

Configuration Steps

↘ Running (no) all-guard enable in Global Configuration Mode

Verification

When a host sends a large number of packets corresponding to basic guards to a switch, such as ARP/ICMP packets, NFPP guard detection takes effect by default.

- Run the **no all-guard enable** command. With the **show cpu-protect** command used, NFPP ratelimit failure is displayed. With the **show nfpp xx-guard host** command used, no attacker is displayed. With the **show nfpp xx-guard summary** command used, the "disabled" status of guards is displayed.

Related Commands

Configuration Example

↘ Prioritizing Packets Sent to the CPU Through Centralized Bandwidth Allocation

Scenario	● N/A
Configuration Steps	● N/A
	Hostname(config)#show running-config | begin nfpp nfpp log-buffer enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 ! Hostname(config)# nfpp Hostname(config-nfpp)#no all-guard enable Hostname(config-nfpp)#show running-config | begin nfpp nfpp log-buffer enable no arp-guard enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 no icmp-guard enable

	no ip-guard enable no dhcp-guard enable no dhcpv6-guard enable no nd-guard enable ! Hostname(config-nfpp)#all-guard enable Hostname(config-nfpp)#show running-config | begin nfpp nfpp log-buffer enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 ! no service password-encryption !
Verification	N/A

Common Errors

N/A

15.4.10 Configuring NFPP Logging

Configuration Effect

- NFPP obtains a log from the dedicated log buffer at a certain rate, generates a system message, and clears this log from the dedicated log buffer.

Notes

- Logs are continuouslyprinted in the log buffer, even if attacks have stopped.

Configuration Steps

↘ Configuring the Log Buffer Size

- Mandatory.
- If the log buffer is full, new logs replace the old ones.
- If the log buffer overflows, subsequent logs replace the previous ones with all attributes marked with a hyphen (-) is displayed in the log buffer. The administrator needs to increase the log buffer size or the system message generation rate.

Configuring the Log Buffer Rate

- Mandatory.
- The log buffer rate depends on two parameters: the time period and the number of system messages generated in the time period.
- If both of the preceding two parameters are set to 0, system messages are immediately generated for logs but are not stored in the log buffer.

Enabling Log Filtering

- (Optional) Log filtering is disabled by default.
- Logs can be filtered based on an interface or VLAN.
- If log filtering is enabled, logs not meeting the filtering rule are discarded.

Enabling Log Printing

- (Mandatory) Logs are stored in the buffer by default.
- If you want to monitor attacks in real time, you can configure logs to be printed on the screen to export the log information in real time.

Verification

Check whether the configuration takes effect based on the log configuration and the number and interval of printed logs.

Related Commands

Configuring the Log Buffer Size

Command	**log-buffer entries** *number*
Parameter Description	*number*: Indicates the buffer size in the unit of the number of logs, ranging from 0 to 1,024.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Log Buffer Rate

Command	**log-buffer logs** *number_of_message* **interval** *length_in_seconds*
Parameter Description	*number_of_message*: Ranges from 0 to 1,024. The value 0 indicates that all logs are recorded in the log buffer and no system message is generated. *length_in_seconds*: Ranges from 0 to 86,400 (1 day). The value 0 indicates that logs are not recorded in the log buffer but system messages are instantly generated. This also applies to *number_of_message* and *length_in_seconds*. *number_of_message/length_in_second* indicates the system message generation rate.
Command	NFPP configuration mode

Mode	
Usage Guide	N/A

Configuring VLAN-based Log Filtering

Command	**logging vlan** *vlan-range*
Parameter Description	*vlan-range*: Records logs in a specified VLAN range. The value format is 1-3,5 for example.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs in the specified VLAN range are recorded. Between interface-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Configuring Interface-based Log Filtering

Command	**logging interface** *interface-id*
Parameter Description	*interface-id*: Records logs of a specified interface.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs of the specified interface are recorded. Between interface-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Enabling Log Printing

Command	**log-buffer enable**
Parameter Description	N/A
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuration Example

Configuring NFPP Logging

Scenario	● If attackers are too many, log printing will affect the usage of user interfaces, which requires restriction.
Configuration Steps	● Configure the log buffer size. ● Configure the log buffer rate. ● Configure VLAN-based log filtering.
	Hostname# configure terminal Hostname(config)# nfpp

	Hostname (config-nfpp)#log-buffer entries 1024 Hostname (config-nfpp)#log-buffer logs 3 interval 5 Hostname (config-nfpp)#logging interface vlan 1
Verification	● Run the **show nfpp log summary** command to display the configuration.
	Total log buffer size : 1024 Syslog rate : 3 entry per 5 seconds Logging: VLAN 1
	● Run the **show nfpp log buffer** command to display logs in the log buffer.
	Protocol VLAN Interface IP address MAC address Reason Timestamp -------- ---- --------- ---------- ---------- ------ --------- ARP 1 Gi0/5 192.168.206.2 001a.a9c2.4609 SCAN 2013-5-1 5:4:24

15.5 Monitoring

Clearing

Description	Command
Clears the ARP-guard scanning table.	**clear nfpp arp-guard scan**
Clears ARP-guard monitored hosts.	**clear nfpp arp-guard hosts**
Clears IP-guard monitored hosts.	**clear nfpp ip-guard hosts**
Clears ND-guard monitored hosts.	**clear nfpp nd-guard hosts**
Clears ICMP-guard monitored hosts.	**clear nfpp icmp-guard hosts**
Clears DHCP-guard monitored hosts.	**clear nfpp dhcp-guard hosts**
Clears DHCPv6-guard monitored hosts.	**clear nfpp dhcpv6-guard hosts**
Clears self-defined guard monitored hosts.	**clear nfpp define** *name* **hosts**
Clears NFPP logs.	**clear nfpp log**

Displaying

Description	Command
Displays ARP-guard configuration.	**show nfpp arp-guard summary**
Displays ARP-guard monitored hosts.	**show nfpp arp-guard hosts**
Displays the ARP-guard scanning table.	**show nfpp arp-guard scan**
Displays IP-guard configuration.	**show nfpp ip-guard summary**
Displays IP-guard monitored hosts.	**show nfpp ip-guard hosts**
Displays the IP-guard scanning table.	**show nfpp ip-guard trusted-host**
Displays ICMP-guard configuration.	**show nfpp icmp-guard summary**

Description	Command
Displays ICMP-guard monitored hosts.	**show nfpp icmp-guard hosts**
Displays the ICMP-guard scanning table.	**show nfpp icmp-guard trusted-host**
Displays DHCP-guard configuration.	**show nfpp dhcp-guard summary**
Displays DHCP-guard monitored hosts.	**show nfpp dhcp-guard hosts**
Displays DHCPv6-guard configuration.	**show nfpp dhcpv6-guard summary**
Displays DHCPv6-guard monitored hosts.	**show nfpp dhcpv6-guard hosts**
Displays ND-guard configuration.	**show nfpp nd-guard summary**
Displays self-defined guard configuration.	**show nfpp define summary** [*name*]
Displays the monitored hosts.	**show nfpp define hosts** *name*
Displays the trusted hosts.	**show nfpp define trusted-host** *name*
Displays NFPP logs.	**show nfpp log summary**
Displays the NFPP log buffer.	**show nfpp log buffer** [**statistics**]

ACL & QoS Configuration

1. Configuring ACL
2. Configuring QoS

1 Configuring the ACL

1.1 Overview

Access control list (ACL) is also called access list or firewall. It is even called packet filtering in some documents. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

ACLs are classified by function into two types:

- Security ACLs: Used to control data flows that are allowed to pass through a network device.
- Quality of service (QoS) ACLs: Used to classify and process data flows by priority.

ACLs are configured for a lot of reasons. Major reasons include:

- Network access control: To ensure network security, rules are defined to limit access of users to some services (for example, only access to the WWW and email services is permitted, and access to other services such as Telnet is prohibited), or to allow users to access services in a specified period of time, or to allow only specified hosts to access the network.
- QoS: QoS ACLs are used to preferentially classify and process important data flows. For details about the use of QoS ALCs, see the configuration manual related to QoS.

1.2 Applications

Application	Description
Access Control of an Enterprise Network	On an enterprise network, the network access rights of each department, for example, access rights of servers and use permissions of chatting tools (such as QQ and MSN), must be controlled according to requirements.

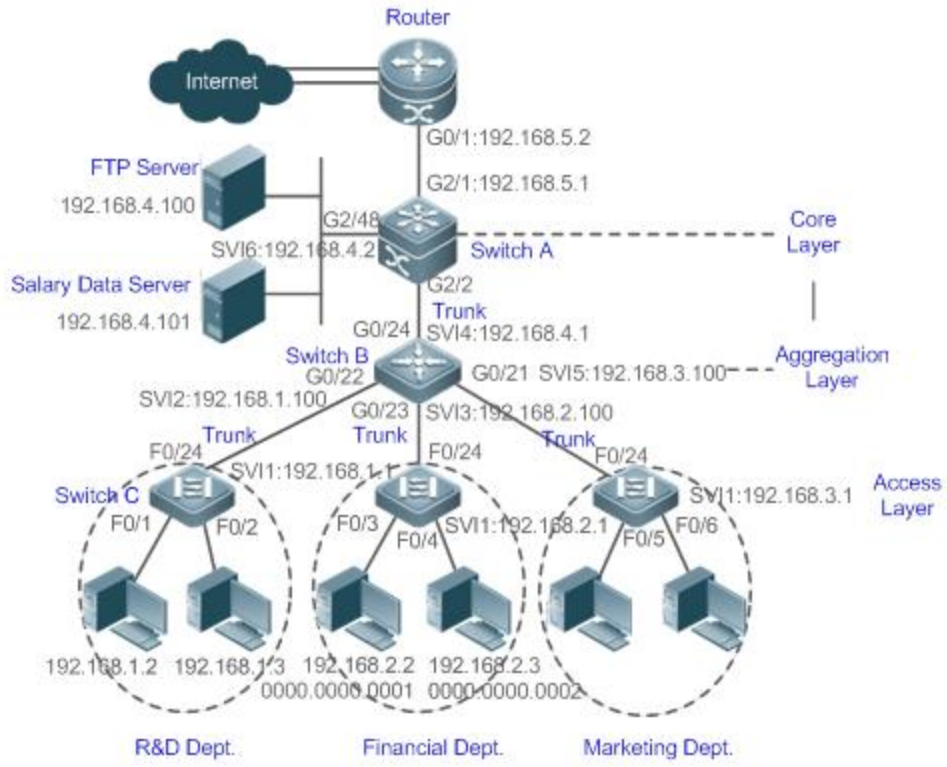
1.2.1 Access Control of an Enterprise Network

Scenario

Internet viruses can be found everywhere. Therefore, it is necessary to block ports that are often used by viruses to ensure security of an enterprise network as follows:

- Allow only internal PCs to access the server.
- Prohibit PCs of a non-financial department from accessing PCs of the financial department, and prohibit PCs of a non-R&D department from accessing PCs of the R&D department.
- Prohibit the staff of the R&D department from using chatting tools (such as QQ and MSN) during working hours from 09:00 to 18:00.

Figure 1-1



Remarks	Switch C at the access layer:It is connected to PCs of each department and to Switch B at the aggregation layer through the gigabit optical fiber (trunk mode). Switch B at the aggregation layer:Multiple virtual local area networks (VLANs) are divided. One VLAN is defined for one department. These VLANs are connected to Switch A at the core layer through the 10-gigabit optical fiber (trunk mode). Switch A at the core layer:It is connected to various servers, such as the File Transfer Protocol (FTP) server and Hypertext Transfer Protocol (HTTP) server, and to the Internet through firewalls.

Deployment

- Configure an extended ACL on the port G2/1 to filter data packets, thus protecting the network against the viruses. This port is located on a core-layer device (Switch A) and used to connect Switch A to the uplink port G2/1 of a router.
- Allow only internal PCs to access servers, and prohibit external PCs from accessing servers. Define and apply the extended IP ACLs on G2/2 or switch virtual interface (SVI) 2 that is used to connect Switch A to an aggregation layer device or server.
- Prohibit mutual access between specified departments. Define and apply the extended IP ACLs on G0/22 and G0/23 of Switch B.
- Configure and apply the time-based extended IP ACLs on SVI 2 of Switch B to prohibit the R&D department from using chatting tools (such as QQ and MSN) in a specified period of time.

1.3 Features

Basic Concepts

ACL

ACLs include basic ACLs and dynamic ACLs.

You can select basic or dynamic ACLs as required. Generally, basic ACLs can meet the security requirements. However, experienced hackers may use certain software to access the network by means of IP address spoofing. If dynamic ACLs are used, users are requested to pass identify authentication before accessing the network, which prevents hackers from intruding the network. Therefore, you can use dynamic ACLs in some sensitive areas to guarantee network security.

IP address spoofing is an inherent problem of all ACLs, including dynamic ACLs. Hackers may use forged IP addresses to access the network during the validity period of authenticated user identities. Two methods are available to resolve this problem. One is to set the idle time of user access to a smaller value, which increases the difficulty in intruding networks. The other is to encrypt network data using the IPSec protocol, which ensures that all data is encrypted when arriving at a device.

ACLs are generally configured on the following network devices:

- Devices between the internal network and the external network (such as the Internet)
- Devices on the border of two network segments
- Devices connected to controlled ports

ACL statements must be executed in strict compliance with their sequence in the ACL. Comparison starts from the first statement. Once the header of a data packet matches a statement in the ACL, the subsequent statements are ignored and no longer checked.

Input/Output ACLs, Filtering Field Template, and Rules

When receiving a packet on an interface, the device checks whether the packet matches any access control entry (ACE) in the input ACL of this interface. Before sending a packet through a interface, the device checks whether the packet matches any ACE in the output ACL of this interface.

When different filtering rules are defined, all or only some rules may be applied simultaneously. If a packet matches an ACE, this packet is processed according to the action policy (permit or deny) defined in this ACE. ACEs in an ACL identify Ethernet packets based on the following fields in the Ethernet packets:

Layer 2 (L2) fields:

- 48-bit source MAC address (containing all 48 bits)
- 48-bit destination MAC address (containing all 48 bits)
- 16-bit L2 type field

Layer 3 (L3) fields:

- Source IP address field (All source IP address values can be specified, or the subnet can be used to define a type of data flows.)
- Destination IP address field (All destination IP address values can be specified, or the subnet can be us ed to define a type of data flows.)
- Protocol type field

Layer 4 (L4) fields:

- Either a TCP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.
- Either a UDP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.

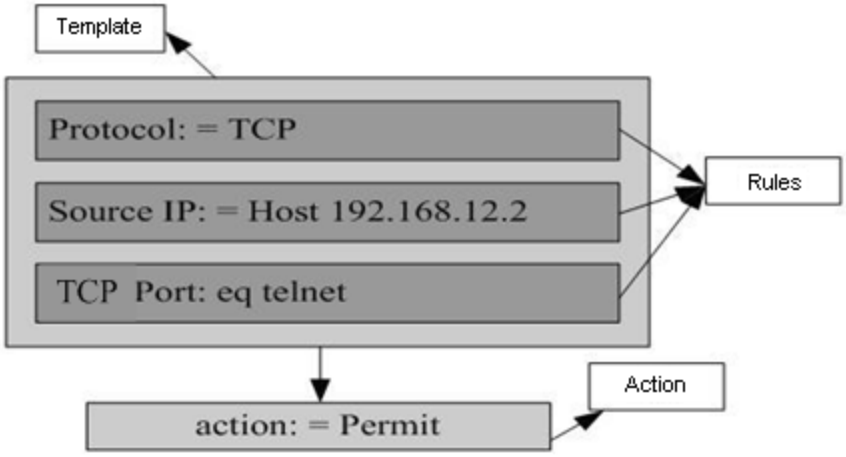
Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field in each packet; when another ACE is generated, packets are identified and classified based on the source IP address field and UDP source port field in each packet. The two ACEs use different filtering field templates.

Rules refer to values of fields in the filtering field template of an ACE. For example, the content of an ACE is as follows:

permit tcp host *192.168.12.2* any eq telnet

In this ACE, the filtering field template is a combination of the following fields: source IP address field, IP protocol field , and TCP destination port field. The corresponding values (rules) are as follows: source IP address = Host 192.168.12.2; IP protocol = TCP; TCP destination port = Telnet.

Figure 1-2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



A filtering field template can be a combination of L3 and L4 fields, or a combination of multiple L2 fields. The filtering field template of a standard or an extended ACL, however, cannot be a combination of L2 and L3 fields, a combination

of L2 and L4 fields, or a combination of L2, L3, and L4 fields. To use a combination of L2,L3, and L4 fields, you can use the expert ACLs.

- An SVI associated with ACLs in the outgoing direction supports the IP standard, IP extended, MAC extended, and expert ACLs.
- If an MAC extended or expert ACL is configured to match the destination MAC address and is applied to the outgoing direction of the SVI, the related ACE can be configured but cannot take effect. If an IP extended or expert ACL is configured to match the destination IP address, but the destination IP address is not in the subnet IP address range of the associated SVI, the configured ACL cannot take effect. For example, assume that the address of VLAN 1 is **192.168.64.1 255.255.255.0**, an IP extended ACL is created, and the ACE is **deny udp any 192.168.65.1 0.0.0.255 eq 255**. If this ACL is applied to the outgoing interface of VLAN 1, the ACL cannot take effect because the destination IP address is not in 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 can take effect because the destination IP address is in the subnet IP address range of VLAN 1.
- On a switch, if ACLs are applied to the outgoing direction of a physical port or an aggregate port (AP), the ACLs can filter only well-known packets, but not unknown unicast packets. That is, for unknown or broadcast packets, ACLs configured in the outgoing direction of a port does not take effect.
- On a switch, if the input ACL and DOT1X, global IP+MAC binding, port security, and IP source guard are shared among all ports, the permit and default deny ACEs do not take effect, but other deny ACEs take effect.
- On a switch, if the input ACL and QoS are shared, the permit ACEs do not take effect, other deny ACEs take effect, and the default deny ACE takes effect after the QoS ACE takes effect.
- On a switch, you can run the **no rgos-security compatible** command to make the permit and deny ACEs take effect at the same time when the port-based input ACL and DOT1X, global IP+MAC binding, port security, and IP source guard are shared.
- If ACEs are added to an ACL and then the switch is restarted after an ACL is applied to the incoming direction of multiple SVIs, the ACL may fail to be configured on some SVIs due to the limited hardware capacity.
- If an expert ACL is configured and applied to the outgoing direction of an interface, and some ACEs in this ACL contain the L3 matching information (e.g. the IP address and L4 port), non-IP packets sent to the device from this interface cannot be controlled by the permit and deny ACEs in this ACL.

ACL Logging

To allow users better learn the running status of ACLs on a device, you can determine whether to specify the ACL logging option as required when adding ACEs. If this option is specified, logs are output when packets matching ACEs are found. ACL logs are displayed based on ACEs. That is, the device periodically displays ACEs with matched packets and the number of matched packets. An example of the log is as follows:

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

To control the amount of logs and output frequency, you can configure the log update interval respectively for the IPv4 ACL and the IPv6 ACL.

- An ACE containing the ACL logging option consumes more hardware resources. If all configured ACEs contain this option, the ACE capacity of a device will be reduced by half.

By default, the log update interval is 0, that is, no log is output. After the ACL logging option is specified in an ACE, you need to configure the log update interval to output related logs.

For an ACE containing the ACL logging option, if no packet is matched in the specified interval, no packet matching log related to this ACE will be output. If matched packets are found in the specified interval, packet matching logs related to this ACE will be output when the interval expires. The number of matched packets is the total number of packets that match the ACE during the specified interval, that is, the period from the previous log output to the current log output.

ACL Packet Matching Counters

To implement network management, users may want to know whether an ACE has any matched packets and how many packets are matched. ACLs provide the ACE-based packet matching counters. You can enable or disable packet matching counters for all ACEs in an ACL, which can be an IP ACL, MAC ACL, expert ACL, or IPv6 ACL. In addition, you can run the **clear counters access-list** [*acl-id* | *acl-name*] command to reset ACL counters for a new round of statistics.

Enabling ACL counters requires more hardware entries. In an extreme case, this will reduce by half the number of ACEs that can be configured on a device.

Overview

Feature	Description
IP ACL	Control incoming or outgoing IPv4 packets of a device based on the L3 or L4 information in the IPv4 packet header.
MAC Extended ACL	Control incoming or outgoing L2 packets of a device based on the L2 information in the Ethernet packet header.
Expert Extended ACL	Combine the IP ACL and MAC extended ACL into an expert extended ACL, which controls (permits or denies) incoming or outgoing packets of a device using the same rule based on the L2, L3, and L4 information in the packet header.
IPv6 ACL	Control incoming or outgoing IPv6 packets of a device based on the L3 or L4 information in the IPv6 packet header.
ACL80	Customize the matching fields and mask for scenarios where fixed matching fields cannot meet the requirements.
ACL Redirection	Redirect incoming packets of a device that match ACEs to a specified outgoing interface.
Global Security ACL	Make an ACL take effect in the incoming direction of all interfaces, instead of applying the ACL on every interface.
Security Channel	Allow packets to bypass the check of access control applications, such as DOT1X and Web authentication, to meet requirements of some special scenarios.
SVI Router ACL	Enable users in the same VLAN to communicate with each other.
ACL Logging	Output ACL packet matching logs at a specified interval according to requirements. The logs help users learn the packet matching result of a specified ACE.

1.3.1 IP ACL

The IP ACL implements refined control on incoming and outgoing IPv4 packets of a device. You can permit or deny the entry of specific IPv4 packets to a network according to actual requirements to control access of IP users to network resources.

Working Principle

Define a series of IP access rules in the IP ACL, and then apply the IP ACL either in the incoming or outgoing direction of an interface or globally. The device checks whether the incoming or outgoing IPv4 packets match the rules and accordingly forwards or blocks these packets.

To configure an IP ACL, you must specify a unique name or ID for the ACL of a protocol so that the protocol can uniquely identify each ACL. The following table lists the protocols that can use IDs to identify ACLs and the range of IDs.

Protocol	ID Range
Standard IP	1–99, 1300–1999
Extended IP	100–199, 2000–2699

Basic ACLs include the standard IP ACLs and extended IP ACLs. Typical rules defined in an ACL contain the following matching fields:

- Source IP address
- Destination IP address
- IP protocol number
- L4 source port ID or ICMP type
- L4 destination port ID or ICMP code

The standard IP ACL (ID range: 1–99, 1300–1999) is used to forward or block packets based on the source IP address, whereas the extended IP ACL (ID range: 100–199, 2000–2699) is used to forward or block packets based on a combination of the preceding matching fields.

For an individual ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

↘ Implicit "Deny All Traffic" Rule Statement

At the end of every IP ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 1 permit host 192.168.4.12
```

This ACL permits only packets sent from the source host 192.168.4.12, and denies packets sent from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 1 deny any**.

If the ACL contains only the following statement:

```
access-list 1 deny host 192.168.4.12
```

Packets sent from any host will be denied when passing through this port.

When defining an ACL, you must consider the routing update packets. As the implicit "deny all traffic" statement exists at the end of an ACL, all routing update packets may be blocked.

Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and denies all traffic, all subsequent statements will not be checked.

For example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

The first rule statement denies all IP packets. Therefore, Telnet packets from the host on the network 192.168.12.0/24 will be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

Configuring an IP ACL

By default, no IP ACL is configured on a device.

Run the **ip access-list { standard | extended } {*acl-name* | *acl-id*}** command in global configuration mode to create a standard or an extended IP ACL and enter standard or extended IP ACL mode.

Adding ACEs to an IP ACL

By default, a newly created IP ACL contains an implicit ACE that denies all IPv4 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv4 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv4 packets, add some ACEs to the ACL.

For a standard IP ACL, add ACEs as follows:

- No matter whether the standard IP ACL is a named or number ACL, you can run the following command in standard IP ACL mode to add an ACE:
  [*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]
- For a numbered standard IP ACL, you can also run the following command in global configuration mode to add an ACE:
  access-list *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*][**log**]

For an extended IP ACL, you can add ACEs as follows:

- No matter whether the extended IP ACL is a named or numbered ACL, you can run the following command in extended IP ACL mode to add an ACE:

[*sn*] { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*] [**log**]

- For a numbered extended IP ACL, you can also run the following command in global configuration mode to add an ACE: **access-list** *acl-id* { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*] [**log**]

Applying an IP ACL

By default, the IP ACL is not applied to any interface, that is, the IP ACL does not filter incoming or outgoing IP packets of the device.

Run the **ip access-group** { *acl-id* **|** *acl-name* } **in** command in interface configuration mode to apply a standard or an extended IP ACL to a specified interface.

1.3.2 MAC Extended ACL

The MAC extended ACL implements refined control on incoming and outgoing packets based on the L2 header of packets. You can permit or deny the entry of specific L2 packets to a network, thus protecting network resources against attacks or control users' access to network resources.

Working Principle

Define a series of MAC access rules in the MAC extended ACL, and then apply the ACL to the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an MAC extended ACL, you must specify a unique name or ID for this ACL to uniquely identify the ACL. The following table lists the range of IDs that identify MAC extended ACLs.

Protocol	ID Range
MAC extended ACL	700–799

Typical rules defined in an MAC extended ACL include:

- Source MAC address
- Destination MAC address
- Ethernet protocol type

The MAC extended ACL (ID range: 700–799) is used to filter packets based on the source or destination MAC address and the Ethernet type in the packets.

For an individual MAC extended ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

If ACEs in an MAC extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the MAC extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

Implicit "Deny All Traffic" Rule Statement

At the end of every MAC extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 700 permit host 00d0.f800.0001 any
```

This ACL permits only packets from the host with the MAC address 00d0.f800.0001, and denies packets from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 700 deny any any**.

Related Configuration

Configuring an MAC Extended ACL

By default, no MAC extended ACL is configured on a device.

Run the **mac access-list extended {*acl-name* | *acl-id* }** command in global configuration mode to create an MAC extended ACL and enter MAC extended ACL mode.

Adding ACEs to an MAC Extended ACL

By default, a newly created MAC extended ACL contains an implicit ACE that denies all L2 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

You can add ACEs to an MAC extended ACL as follows:

- No matter whether the MAC extended ACL is a named or numbered ACL, you can run the following command in MAC extended ACL mode to add an ACE:
  [*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr* | *src-mac-addrmask*}{**any** | **host** *dst-mac-addr* | *dst-mac-addr mask*} [*ethernet-type*] [**cos** *cos*] [**inner** *cos*] [**time-range** *tm-rng-name*]
- For a numbered MAC extended ACL, you can also run the following command in global configuration mode to add an ACE:
  access-list *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr* | *src-mac-addr mask* }{**any** | **host** *dst-mac-addr* | *dst-mac-addr mask* } [*ethernet-type*] [**cos** *cos*] [**inner** *cos*] [**time-range** *time-range-name*]

Applying an MAC Extended ACL

By default, the MAC extended ACL is not applied to any interface, that is, the created MAC extended ACL does not filter incoming or outgoing L2 packets of a device.

Run the **mac access-group** { *acl-id* | *acl-name* } **{ in| out }** command in interface configuration mode to apply an MAC extended ACL to a specified interface

1.3.3 Expert Extended ACL

You can create an expert extended ACL to match the L2 and L3 information in packets using the same rule. The expert extended ACL can be treated as a combination and enhancement of the IP ACL and the MAC extended ACL because the expert extended ACL can contain ACEs in both the IP ACL and the MAC extended ACL. In addition, the VLAN ID can be specified in the expert extended ACL to filter packets.

Working Principle

Define a series of access rules in the expert extended ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an expert extended ACL, you must specify a unique name or ID for this ACL so that the protocol can uniquely identify each ACL. The following table lists the ID range of the expert extended ACL.

Protocol	ID Range
Expert extended ACL	2700–2899

When an expert extended ACL is created, defined rules can be applied to all packets. The device determines whether to forward or block packets by checking whether packets match these rules.

Typical rules defined in an expert extended ACL include:

- All information in the basic ACL and MAC extended ACL
- VLAN ID

The expert extended ACL (ID range: 2700–2899) is a combination of the basic ACL and MAC extended ACL, and can filter packets based on the VLAN ID.

For an individual expert extended ACL, multiple independent statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL.

If rules in an expert extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the expert extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

Implicit "Deny All Traffic" Rule Statement

At the end of every expert extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 2700 permit 0x0806 any any any any any
```

This ACL permits only ARP packets whose Ethernet type is 0x0806, and denies all other types of packets. This is because the following statement exists at the end of this ACL: **access-list 2700 deny any any any any**.

Related Configuration

Configuring an Expert Extended ACL

By default, no expert extended ACL is configured on a device.

Run the **expert access-list extended {*acl-name* | *acl-id* }** command in global configuration mode to create an expert extended ACL and enter expert extended ACL mode.

↘ Adding ACEs to an Expert Extended ACL

By default, a newly created expert extended ACL contains an implicit ACE that denies all packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

You can add ACEs to an expert extended ACL as follows:

- No matter whether the expert extended ACL is a named or numbered ACL, you can run the following command in expert extended ACL mode to add an ACE:

  [*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

- For a numbered expert extended ACL, you can also run the following command in expert extended ACL mode to add an ACE:

  access-list *acl-id* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]

↘ Applying an Expert Extended ACL

By default, the expert extended ACL is not applied to any interface, that is, the created expert extended ACL does not filter incoming or outgoing L2 or L3 packets of a device.

Run the **expert access-group** { *acl-id* | *acl-name* } **in** command in interface configuration mode to apply an expert extended ACL to a specified interface

1.3.4 IPv6 ACL

The IPv6 ACL implements refined control on incoming and outgoing IPv6 packets of a device. You can permit or deny the entry of specific IPv6 packets to a network according to actual requirements to control access of IPv6 users to network resources.

Working Principle

Define a series of IPv6 access rules in the IPv6 ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing IPv6 packets match the rules and accordingly forwards or blocks these packets.

To configure an IPv6 ACL, you must specify a unique name for this ACL.

Unlike the IP ACL, MAC extended ACL, and expert extended ACL, you can specify only a name but not an ID for the IPv6 ACL created.

Only one IP ACL, or one MAC extended ACL, or one expert extended ACL can be applied to the incoming or outgoing direction of an interface. Besides, one more IPv6 ACL can be applied.

Implicit "Deny All Traffic" Rule Statement

At the end of every IPv6 ACL is an implicit "deny all IPv6 traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
ipv6 access-list ipv6_acl
 10 permit ipv6 host 200::1 any
```

This ACL permits only IPv6 packets from the source host 200::1, and denies IPv6 packets from all other hosts. This is because the following statement exists at the end of this ACL: deny ipv6 any any.

Although the IPv6 ACL contains the implicit "deny all IPv6 traffic" rule statement by default, it does not filter ND packets.

Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and permits all IPv6 traffic, all subsequent statements will not be checked.

For example:

```
ipv6 access-list ipv6_acl
10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

As the first rule statement permits all IPv6 packets, all IPv6 packets sent from the host 200::1 does not match the subsequent deny rule with the serial number of 20, and therefore will not be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements anymore.

Related Configuration

Configuring an IPv6 ACL

By default, no IPv6 ACL is configured on a device.

Run the **ipv6 access-list** ***acl-name*** command in global configuration mode to create an IPv6 ACL and enter IPv6 ACL mode.

Adding ACEs to an IPv6 ACL

By default, a newly created IPv6 ACL contains an implicit ACE that denies all IPv6 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv6 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv6 packets, add some ACEs to the ACL.

Run the following command in IPv6 ACL mode to add an ACE:

[*sn*] { **permit** | **deny** } *ipv6-protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* } { *destination-ipv6-prefix/prefix-length* | **any** | *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]

By default, the IPv6 ACL is not applied to any interface, that is, the IPv6 ACL does not filter incoming or outgoing IPv6 packets of a device.

Run the **ipv6 traffic-filter** *acl-name* **in** command in interface configuration mode to apply an IPv6 ACL to a specified interface.

1.3.5 ACL80

ACL80 refers to the expert advanced ACL, and is also called custom ACL. It filters packets based on the first 80 bytes of every packet. Among these 80 bytes, the SMAC, DMAC, SIP, DIP, and ETYPE fields in a packet are mandatory, and you can specify the remaining 16 bytes.

Working Principle

A packet consists of a number of bytes. ACL80 allows you to match the specified 16 bytes by bit in the first 80 bytes of a packet. Any bit of a 16-byte field can be set to a value (**0** or **1**), indicating whether the bit is compared. When any byte is filtered, three factors are considered: content of the matching field, mask of the matching field, and the start position for matching. Bits of the matching field content are in one-to-one mapping relationship with bits of the matching field mask. The filtering rule specifies the value of the field to be filtered. The filtering field template specifies whether the corresponding field in the filtering rule should be filtered. (**1** indicates that the bit specified in the filtering rule should be matched; **0** indicates that the bit specified in the filtering rule is not matched.) Therefore, when it is required to match a specific bit, you must set the corresponding bit to 1 in the filtering field template. For example, if the bit is set to **0** in the filtering field template, no bit is matched no matter which bit is specified in the filtering rule.

For example,

```
Hostname(config)#expert access-list advanced name
Hostname(config-exp-dacl)#permit 00d0f8123456 ffffffffffff 0
Hostname(config-exp-dacl)#deny 00d0f8654321 ffffffffffff 6
```

The custom ACL matches any byte of the first 80 bytes in a L2 data frame according to user' definition, and filters packets accordingly. To properly use a custom ACL, you must have an in-depth understanding about the structure of a L2 data frame. The following shows the first 64 bytes of a L3 data frame (every letter represents a hexadecimal number, and every two letters represent one byte):

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

The following table describes the meaning and offset of each letter:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC address	0	O	Time To Live (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	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	Cntl 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 number	26	XY	IP header length and reserved bit	58
K	TOS field	27	Z	Reserved bit and flags bit	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Miscellaneous	62
N	Flags field	32			

In the above table, the offset of each field is the offset of this field in the tagged 802.3 SNAP packet. In a custom ACL, you can use the rule mask and offset jointly to extract any byte from the first 80 bytes of a data frame, compare the byte with the rule customized in the ACL, and then filter matched data frames for further processing. Customized rules may be some fixed attributes of data. For example, to obtain all TCP packets, you can define the rule as "06", rule mask as "FF", and offset as "35". Then, the device can use the rule mask and offset jointly to extract the content of TCP protocol number field in a received data frame, and compare the extracted content with the rule to obtain all TCP packets.

The ACL80 supports filtering of the Ethernet, 803.3 SNAP, and 802.3 LLC packets. If the values of the fields from DSAP to cntl are set to AAAA03, the ACL is used to filter the 803.3 SNAP packets. If the values of the fields from DSAP to cntl are set to E0E003, the ACL is used to filter the 803.3 LLC packets. The value of the cntl field cannot be configured to filter Ethernet packets.

The ACL80 can be configured to compare packets with any of the 16 bytes. If the 16 bytes are already used, no ACE can be configured to compare packets with fields in any other bytes.

Related Configuration

Configuring an Expert Advanced ACL

By default, no expert advanced ACL is configured on a device.

Run the **expert access-list advanced *acl-name*** command in global configuration mode to create an expert advanced ACL and enter expert advanced ACL mode.

Adding ACEs to an Expert Advanced ACL

By default, a newly created expert advanced ACL contains an implicit ACE that denies all packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

- Run the [*sn*] { **permit** | **deny** } *hex hex-mask offset* command in expert advanced ACL mode to add an ACE to the expert advanced ACL.

Applying an Expert Advanced ACL

By default, the expert advanced ACL is not applied to any interface, that is, the created expert advanced ACL does not filter incoming or outgoing packets of a device.

Run the **expert access-group** *acl-name* **in** command in interface configuration mode to apply an expert advanced ACL to a specified interface.

1.3.6 ACL Redirection

ACL redirection allows a device to analyze received packets and redirect the packets to a specified port for forwarding. To analyze specific incoming packets of a device, you can configure the ACL redirection function to redirect packets meeting rules to a specified port and capture packets on this port for analysis.

Working Principle

Bind different ACL policy to an interface and specify an output destination interface for each policy. When receiving packets on this interface, the device searches ACL policies bound to this interface one by one. If packets match criteria described in a certain policy, the device forwards packets on the destination interface specified by the policy, thus redirecting packets based on traffic.

ACL redirection takes effect only in the incoming direction of an interface.

Related Configuration

Configuring an ACL

Before configuring ACL redirection, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring ACL Redirection

By default, ACL redirection is not configured on a device.

Run the **redirect destination interface** *interface-name* **acl** {*acl-id* | ***acl-name*** } **in** command in interface configuration mode to configure ACL redirection.

You can configure the ACL redirection function only on an Ethernet interface, AP, or SVI.

1.3.7 Global Security ACL

To meet the requirements of security deployment, the port-based ACL is often configured to filter out virus packets and obtain packets with certain characteristics, for example, packets that attack the TCP port. Various virus packets exist in a global network environment, and the identification features of virus packets under each port are identical or similar. Therefore, an ACL is generally created. After the deny ACE for matching virus signatures is added to the ACL, the port-based ACL is applied to each port on the switch to filter out virus packets.

For two reasons, it is not convenient to use the port-based ACLs in antivirus scenarios such as virus filtering. The first reason is that the port-based ACL must be configured on every port, which results in repeated configuration, poor operation performance, and over-consumption of ACL resources. The second reason is that the access control function of the ACL is weakened. As the port-based ACL is used for virus filtering, basic functions of the ACL, such as route update restriction and network access restriction, cannot be used properly. The global security ACL can be used for global antivirus deployment and defense without affecting the port-based ACL. By running only one command, you can make the global security ACL takes effect on all L2 interfaces. In contrast, the port-based ACL must be configured on every interface.

Working Principle

The global security ACL takes effect on all L2 interfaces. When both the global security ACL and the port-based ACL are configured, both take effect. Packets that match the global security ACL are directly filtered out as virus packets. Packets that do not match the global security ACL are still controlled by the port-based ACL. You can disable the global security ACL on some ports so that these ports are not controlled by the global security ACL.

- The global security ACL is mainly used for virus filtering. Therefore, in an ACL associated with the global security ACL, only the deny ACEs take effect, and the permit ACEs do not take effect.
- Unlike the secure ACL applied to a port, the global security ACL does not contain the default "deny all traffic" ACE, that is, all packets that do not match the ACL are permitted.
- A global secure ACL can take effect either on a L2 port or a routed port.
- You can disable the global security ACL on an individual physical port or AP, but not on a member port of an AP.
- The global secure ACL supports only the associated IP standard ACL, IP extended ACL, MAC extended ACL and Expert extended ACL.

Related Configuration

Configuring an ACL

Before configuring the global security ACL, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL.

Configuring a Global Security ACL

By default, no global security ACL is configured on a device.

Run the {**ip |mac** | **expert** } **access-group** *acl-id* **in** command in global configuration mode to enable the global security ACL.

Configuring an Exclusive Interface of the Global Security ACL

By default, no exclusive interface is configured for the global security ACL on a device.

Run the **no global ip access-group** command in interface configuration to disable the global security ACL on a specified interface.

1.3.8 Security Channel

In some application scenarios, packets meeting some characteristics may need to bypass the checks of access control applications. For example, before DOT1X authentication, users are allowed to log in to a specified website to download the DOT1X authentication client. The security channel can be used for this purpose. When the security channel configuration command is executed to apply a secure ACL globally or to an interface, this ACL becomes a security channel.

Working Principle

The security channel is also an ACL, and can be configured globally or for a specified interface. When arriving at an interface, packets are check on the security channel. If meeting the matching conditions of the security channel, packets directly enters a switch without undergoing the access control, such as port security, Web authentication, 802.1x, and IP+MAC binding check. A globally applied security channel takes effect on all interfaces except exclusive interfaces.

- The deny ACEs in an ACL that is applied to a security channel do not take effect. In addition, this ACL does not contain an implicit "deny all traffic" rule statement at the end of the ACL. If packets do not meet matching conditions of the security channel, they are checked according to the access control rules in compliance with the relevant process.
- You can configure up to eight exclusive interfaces for the global security channel. In addition, you cannot configure interface-based security channel on these exclusive interfaces.
- If a security channel is applied to an interface while a global security channel exists, this global security channel does not take effect on this interface.
- If both port-based migratable authentication mode and security channel are applied to an interface, the security channel does not take effect.
- An IPv6 ACL cannot be configured as a security channel.

Related Configuration

Configuring an ACL

Before configuring the security channel, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, or expert extended ACL.

Configuring a Security Channel on an Interface

By default, no security channel is configured on an interface of a device.

Run the **security access-group** {*acl-id* | ***acl-name*** } command in interface configuration mode to configure the security channel on an interface.

Configuring a Global Security Channel

By default, no global security channel is configured on a device.

Run the **security global access-group** {*acl-id* | ***acl-name*** } command in global configuration mode to configure a global security channel.

Configuring an Exclusive Interface for the Global Security Channel

By default, no exclusive interface is configured for the global security channel on a device.

Run the **security uplink enable** command in interface configuration mode to configure a specified interface as the exclusive interface of the global security channel.

1.3.9 SVI Router ACL

By default, an ACL that is applied to an SVI also takes effect on L2 packets forwarded within a VLAN and L3 packets forwarded between VLANs. Consequently, users in the same VLAN may fail to communicate with each other. Therefore, a switchover method is provided so that the ACL that is applied to an SVI takes effect only on routing packets between VLANs.

Working Principle

By default, the SVI router ACL function is disabled, and an SVI ACL takes effect on L3 packets forwarded between VLANs and L2 packets forwarded within a VLAN. After the SVI router ACL function is enabled, the SVI ACL takes effect only on L3 packets forwarded between VLANs.

Related Configuration

Configuring an ACL

Before configuring the SVI router ACL, configure and apply an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL. Apply the ACL in SVI configuration mode.

Configuring the SVI Router ACL

Run the **svi router-acls enable** command in global configuration mode to enable the SVI router ACL so that the ACL that is applied to an SVI takes effect only on packets forwarded at L3, and not on packets forwarded at L2 within a VLAN.

1.3.10 ACL Logging

ACL logging is used to monitor the running status of ACEs in an ACL and provide essential information for routine network maintenance and optimization.

Working Principle

To better learn the running status of ACLs on a device, you can determine whether to specify the ACL logging option as required when adding ACEs. If this option is specified, logs are output when packets matching ACEs are found. ACL logs are displayed based on ACEs. That is, the device periodically displays ACEs with matched packets and the number of matched packets. An example of the log is as follows:

```
*Sep  9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

To control the amount of logs and output frequency, you can configure the log update interval.

- An ACE containing the ACL logging option consumes more hardware resources. If all configured ACEs contain this option, the ACE capacity of a device will be reduced by half.
- By default, the log update interval is 0, that is, no log is output. After the ACL logging option is specified in an ACE, you need to configure the log update interval to output related logs; otherwise, logs are not output.
- For an ACE containing the ACL logging option, if no packet is matched in the specified interval, no packet matching log related to this ACE will be output. If matched packets are found in the specified interval, packet matching logs related to this ACE will be output when the interval expires. The number of matched packets is the total number of packets that match the ACE during the specified interval, that is, the period from the previous log output to the current log output.
- You can configure the ACL logging option only for an IP ACL or an IPv6 ACL.

Related Configuration

Configuring an ACL

Configure an ACL before configuring ACEs containing the ACL logging option. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL. Note that the ACL logging option must be configured.

Configuring the Log Update Interval

Run the {**ip | ipv6**} **access-list log-update inerval** *time* command in the configuration mode to configure the interval at which the ACL logs are output.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL.

1.3.11 Packet Matching Counters

In addition to ACL logs, packet matching counters provide another choice for routine network maintenance and optimization.

Working Principle

To implement network management, users may want to know whether an ACE has any matched packets and how many packets are matched.ACLs provide the ACE-based packet matching counters. You can enable or disable packet matching counters for all ACEs in an ACL. When a packet matches the ACE, the corresponding counter increments by 1. You can run the **clear counters access-list** [*acl-id* | *acl-name*] command to reset counters of all ACEs in an ACL for a new round of statistics.

Enabling ACL counters requires more hardware entries. In an extreme case, this will reduce by half the number of ACEs that can be configured on a device.

You can enable packet matching counters on an IP ACL, MAC ACL, expert ACL, or IPv6 ACL.

Related Configuration

Configuring an ACL

Configure an ACL before configuring ACEs containing the ACL logging option. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL. Note that the ACL logging option must be configured.

Enabling Packet Matching Counters

To enable packet matching counters on an IP ACL, MAC ACL, or expert ACL, run the {**mac | expert** | **ip**} **access-list counter** { *acl-id* | *acl-name* } command in global configuration mode.
To enable packet matching counters on an IPv6 ACL, run the **ipv6 access-list counter** *acl-name* command in global configuration mode.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Clearing Packet Matching Counters

Run the **clear counters access-list** [*acl-id* | *acl-name*] command in privileged EXEC mode to reset packet matching counters.

1.3.12 Fragmented Packet Matching Mode

In fragmented packet matching mode, an ACL can implement more refined control on fragmented packets.

Working Principle

IP packets may be fragmented when transmitted on the network. When fragmentation occurs, only the first fragment of the packet contains the L4 information, such as the TCP/UDP port number, ICMP type, and ICMP code, and other fragmented packets do not contain the L4 information. By default, if an ACE contains the fragment flag, fragmented packets except the first fragments are filtered. If an ACE does not contain the fragment flag, all fragmented packets (including the first fragments) are filtered. In addition to this default fragmented packet matching mode, a new fragmented packet matching mode is provided. You can switch between the two fragmented packet matching modes as required on a specified ACL. In the new fragmented packet matching mode, if an ACE does not contain the fragment flag and packets are fragmented, the first fragments are compared with all the matching fields (including L3 and L4 information) defined in the ACE, and other fragmented packets are compared with only the non-L4 information defined in the ACE.

- In the new fragmented packet matching mode, if an ACE does not contain the fragment flag and the action is Permit, this type of ACE occupies more hardware entries. In an extreme case, this will reduce by half the number of hardware entries. If Established is configured for filter the TCP flag in an ACE, more hardware entries will be occupied.
- The ACL will be temporarily ineffective during switchover of the fragmented packet matching mode.
- In the new fragmented packet matching mode, if an ACE does not contain the fragment flag, the L4 information of packets needs to be compared, and the action is Permit, the ACE checks the L3 and L4 information of the first fragments of packets, and checks only the L3 information of other fragmented packets. If the action is Deny, the ACE checks only the first fragments of packets, and ignores other fragmented packets.
- In the new fragmented packet matching mode, if an ACE contains the fragment flag, the ACE checks only fragmented packets but not the first fragments of packets no matter whether the action in the ACE is Permit or Deny.
- Only the IP extended ACL and the expert extended ACL support switching between the two fragmented packet matching modes.

Related Configuration

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL and expert extended ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and expert extended ACL. Note that the fragment option must be added.

Switching the Fragmented Packet Matching Mode

Run the [**no**] {**ip | expert**} **access-list new-fragment-mode** { *acl-id* | *acl-name* } command in global configuration mode to switch the fragmented packet matching mode.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL and expert extended ACL.

1.4 Configuration

Configuration Item	Description and Command	
Configuring an IP ACL	(Optional) It is used to filter IPv4 packets.	
	ip access-list standard	Configures a standard IP ACL.
	ip access-list extended	Configures an extended IP ACL.
	permit host any time-range log	Adds a permit ACE to a standard IP ACL.
	deny host any time-range log	Adds a deny ACE to a standard IP ACL.
	permit host any host any tos dscp precedence fragment time-range log	Adds a permit ACE to an extended IP ACL.
	deny host any host any tos dscp precedence fragment time-range log	Adds a deny ACE to an extended IP ACL.
	ip access-group in out	Applies a standard or an extended IP ACL.
Configuring an MAC Extended ACL	(Optional) It is used to filter L2 packets.	
	mac access-list extended	Configures an MAC extended ACL.
	permit any host any host cos inner time-range	Adds a permit ACE to an MAC extended ACL.
	deny any host any host cos inner time-range	Adds a deny ACE to an MAC extended ACL.
	mac access-group in out	Applies an MAC extended ACL.
Configuring an Expert Extended ACL	(Optional) It is used to filter L2 and L3 packets.	
	expert access-list extended	Configures an expert extended ACL.
	permit cos inner VID inner host any host any host any precedence tos fragment range time-range	Adds a permit ACE to an expert extended ACL.

Configuration Item	Description and Command	
	deny cos inner VID inner host any host any host any host any precedence tos fragment range time-range	Adds a deny ACE to an expert extended ACL.
	expert access-group in out	Applies an expert extended ACL.
Configuring an IPv6 Extended ACL	(Optional) It is used to filter IPv6 packets.	
	ipv6 access-list	Configures an IPv6 ACL.
	permit host any host any range dscp flow-label fragment time-range	Adds a permit ACE to an IPv6 ACL.
	deny host any host any range dscp flow-label fragment time-range	Adds a deny ACE to an IPv6 ACL.
	ipv6 traffic-filter in out	Applies an IPv6 ACL.
Configuring an ACL80	(Optional) It is used to customize the fields for filter L2 and L3 packets.	
	expert access-list advanced	Configures an expert advanced ACL.
	permit	Adds a permit ACE to an expert advanced ACL.
	deny	Adds a deny ACE to an expert advanced ACL.
	expert access-group in out	Applies an expert advanced ACL
Configuring ACL Redirection	(Optional) It is used to redirect packets meeting the rules to a specified interface.	
	redirect destination interface acl in	Configures ACL redirection.
Configuring a Global Security ACL	(Optional) It is used to make an ACL take effect globally.	
	ip access-group in out	Applies a global security ACL in global configuration mode.
	no global ip access-group	Configures an interface as the exclusive interface of the global security ACL in interface configuration mode.
Configuring a Security Channel	(Optional) It is used to enable packets meeting some characteristics to bypass the checks of access control applications, such as the DOT1X and Web authentication.	
	security access-group	Enables the security channel in interface configuration mode.
	security global access-group	Enables the security channel in global configuration mode.
	security uplink enable	Configures an interface as the exclusive interface of the global security channel in interface configuration mode.

Configuration Item	Description and Command	
Configuring Comments for ACLs	(Optional) It is used to configure comments for an ACL or ACE so that users can easily identify the functions of the ACL or ACE.	
	list-remark	Configures a comment for an ACL in ACL configuration mode.
	access-list list-remark	Configures a comment for an ACL in global configuration mode.
	remark	Configures a comment for an ACE in ACL configuration mode.

1.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface to control all incoming and outgoing IPv4 packets of this interface. You can permit or deny the entry of specific IPv4 packets to a network to control access of IP users to network resources.

Notes

N/A

Configuration Steps

Configuring an IP ACL

- (Mandatory) Configure an IP ACL if you want to control access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IP ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an IP ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv4 packets of the device are denied by default.

Applying an IP ACL

- (Mandatory) Apply an IP ACL to a specified interface if you want this ACL to take effect.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IP ACL:
- Run the **ping** command to verify that the IP ACL takes effect on the specified interface. For example, if an IP ACL is configured to prohibit a host with a specified IP address or hosts in a specified IP address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.

- Access related network resources to verify that the IP ACL takes effect on the specified interface. For example, access the Internet or access the FTP resources on the network through FTP.

Related Commands

Configuring an IP ACL

Command	**ip access-list** { **standard | extended** } {*acl-name* | *acl-id* }
Parameter Description	**standard**: Indicates that a standard IP ACL is created. **extended**: Indicates that an extended IP ACL is created. *acl-name*: Indicates the name of a standard or an extended IP ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID that uniquely identifies a standard or extended IP ACL. If this option is configured, a numbered ACL is created. If a standard IP ACL is created, the value range of *acl-id* is 1–99 and 1300–1999. If an extended IP ACL is created, the value range of *acl-id* is 100–199 and 2000–2699.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a standard or an extended IP ACL and enter standard or extended IP ACL configuration mode. If you want to control access of users to network resources by checking the source IP address of each packet, configure a standard IP ACL. If you want to control access of users to network resources by checking the source or destination IP address, protocol number, and TCP/UDP source or destination port, configure an extended IP ACL.

Adding ACEs to an IP ACL

- Add ACEs to a standard IP ACL.

Use either of the following methods to add ACEs to a standard IP ACL:

Command	[*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect

	only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs in standard IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*] [**log**]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 1300–1999. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in global configuration mode. It cannot be used to add ACEs to a named IP ACL.

- Add ACEs to an extended IP ACL.

Use either of the following methods to add ACEs to an extended IP ACL:

Command	[*sn*] { **permit** | **deny** } { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE.

	deny: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs in extended IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 2000–1999. *sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE.

	protocol: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment: Indicates that only fragmented IP packets except the first fragments are filtered.** **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in extended IP ACL configuration mode .It cannot be used to add ACEs to a named extended IP ACL.

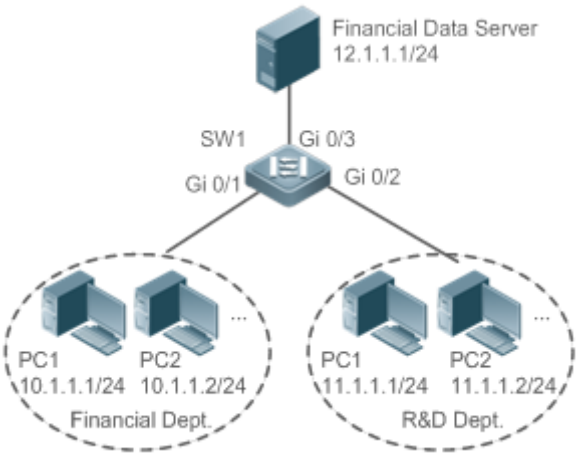
Applying an IP ACL

Command	**ip access-group** { *acl-id* **|** *acl-name* } **in**
Parameter Description	*acl-id*: Indicates that a numbered standard or extended IP ACL will be applied to the interface. *acl-name*: Indicates that a named standard or extended IP ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming IP packets of the interface. **out**: Indicates that this ACL controls outgoing IP packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an IP ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an IP ACL to Prohibit Departments Except the Financial Department from Accessing the Financial Data Server

Scenario **Figure 1-3**	
Configuration Steps	● Configure an IP ACL. ● Add ACEs to the IP ACL. ● Apply the IP ACL to the inbound direction of the interface connecting the financial data server.
SW1	sw1(config)#ip access-list standard 1 sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 in
Verification	● On a PC of the R&D department, ping the financial data server. Verify that the ping operation fails. ● On a PC of the financial department, ping the financial data server. Verify that the ping operation succeeds.
SW1	sw1(config)#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 sw1(config)#show access-group ip access-group 1 in Applied On interface GigabitEthernet 0/3

1.4.2 Configuring an MAC Extended ACL

Configuration Effect

Configure and apply an MAC extended ACL to an interface to control all incoming and outgoing IPv4 packets of this interface. You can permit or deny the entry of specific L2 packets to a network to control access of users to network resources based on L2 packets.

Notes

N/A

Configuration Steps

Configuring an MAC Extended ACL

- (Mandatory) Configure an MAC extended ACL if you want to control users' access to network resources based on the L2 packet header, for example, the MAC address of each user's PC.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The MAC extended ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an MAC Extended ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming L2 Ethernet packets of the device are denied by default.

Applying an MAC extended ACL

- (Mandatory) Apply an MAC extended ACL to a specified interface if you want this ACL take effect.
- You can apply an MAC extended ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the MAC extended ACL:
- If an MAC extended ACL is configured to permit or deny some IP packets, run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, an MAC extended ACL is configured to prevent a device interface from receiving IP packets (Ethernet type is 0x0800), run the **ping** command for verification.
- If an MAC extended ACL is configured to permit or deny some non-IP packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- You can also construct L2 packets meeting some specified characteristics to check whether the MAC extended ACL takes effect. Typically, prepare two PCs, construct and send L2 packets on one PC, enable packet capturing on another PC, and check whether packets are forwarded as expected (forwarded or blocked) according to the action specified in the ACEs.

Related Commands

Configuring an MAC Extended ACL

Command	**mac access-list extended** {*acl-name* | *acl-id* }
Parameter Description	*acl-name*: Indicates the name of an MAC extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID that uniquely identifies an MAC extended ACL. If this option is configured, a numbered ACL is created. The value range of *acl-id* is 700–799.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an MAC extended ACL and enter MAC extended ACL configuration mode. You can configure an MAC extended ACL to control users' access to network resources by checking the L2 information of Ethernet packets.

Adding ACEs to an MAC Extended ACL

Use either of the following methods to add ACEs to an MAC extended ACL:

- Add ACEs in MAC extended ACL configuration mode.

Command	[*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr* | *src-mac-addr mask*} {**any** | **host** *dst-mac-addr* | *dst-mac-addr mask* } [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **any**: Indicates that L2 packets sent from any host are filtered. **host** *src-mac-addr*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. *src-mac-addr mask*: Indicates that the source MAC address is reversed. **any**: Indicates that L2 packets sent to any host are filtered. **host** *dst-mac-addr*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *dst-mac-addr mask*: Indicates that the destination MAC address is reversed. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *cos*: Indicates that L2 packets with the specified class of service (cos) field in the outer tag are filtered. **inner** *cos*: Indicates that L2 packets with the specified cos field in the inner tag are filtered.

	time-range *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	MAC extended ACL configuration mode
Usage Guide	Run this command to add ACEs in MAC extended ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an MAC extended ACL in global configuration mode.

Command	**access-list** *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr* | *src-mac-addr mask* } {**any** | **host** *dst-mac-addr* | *dst-mac-addr mask* } [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 700–799. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *src-mac-addr*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. *src-mac-addr mask*: Indicates that the source MAC address is reversed. **any**: Indicates that L2 packets sent to any host are filtered. **host** *dst-mac-addr*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *dst-mac-addr mask*: Indicates that the destination MAC address is reversed. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *cos*: Indicates that L2 packets with the specified cos field in the outer tag are filtered. **inner** *cos*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered MAC extended ACL in global configuration mode. It cannot be used to add ACEs to a named MAC extended ACL.

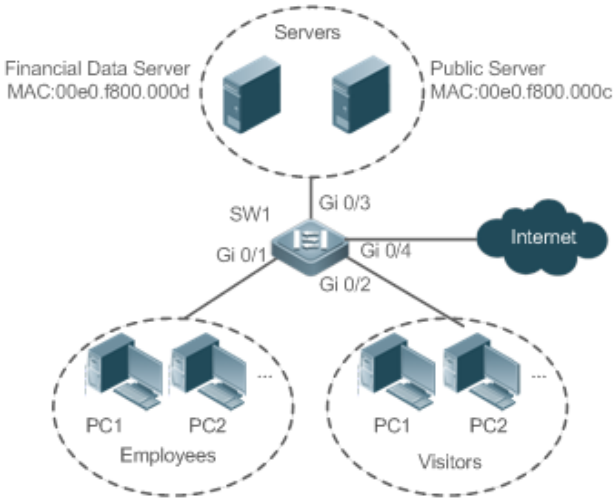
↘ Applying an MAC Extended ACL

Command	**mac access-group** { *acl-id* | *acl-name* } **in**
Parameter Description	*acl-id*: Indicates that a numbered MAC extended IP ACL will be applied to the interface. *acl-name*: Indicates that a named MAC extended IP ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming Layer 2 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an MAC extended ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an MAC Extended ACL to Restrict Resources Accessible by Visitors

Scenario **Figure 1-4**	
Configuration Steps	● Configure an MAC extended ACL. ● Add ACEs to the MAC extended ACL. ● Apply the MAC extended ACL to the outgoing direction of the interface connected to the visitor area so that visitors are allowed to access Internet and the public server of the company, but prohibited from accessing the financial data server of the company. That is, visitors cannot access the server with the MAC address 00e0.f800.000d.
SW1	sw1(config)#mac access-list extended 700 sw1(config-mac-nacl)#deny any host 00e0.f800.000d sw1(config-mac-nacl)#permit any any sw1(config-mac-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in
Verification	● On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ● On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
SW1	sw1(config)#show access-lists mac access-list extended 700

	10 deny any host 00e0.f800.000d etype-any 20 permit any any etype-any sw1(config)#show access-group mac access-group 700 in Applied On interface GigabitEthernet 0/2

1.4.3 Configuring an Expert Extended ACL

Configuration Effect

Configure and apply an expert extended ACL to an interface to control incoming and outgoing packets of the interface based on the L2 and L3 information, and allow or prohibit the entry of specific packets to the network. In addition, you can configure an expert extended ACL to control all L2 packets based on the VLAN to permit or deny the access of users in some network segments to network resources. Generally, you can use an expert extended ACL if you want to incorporate ACEs of the IP ACL and MAC extended ACL into one ACL.

Configuration Steps

Configuring an Expert Extended ACL

- (Mandatory) Configure an expert extended ACL if you want to control users' access to network resources based on the L2 packet header, for example, the VLAN ID.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The expert extended ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an Expert Extended ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming packets of the device are denied by default.

Applying an Expert Extended ACL

- (Mandatory) Apply an expert extended ACL to a specified interface if you want this ACL to take effect.
- You can apply an expert extended ACL in the incoming or outgoing direction of a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the expert extended ACL:
- If IP-based access rules are configured in an expert extended ACL to permit or deny some IP packets, run the **ping** command to verify whether these rules take effect.
- If MAC-based access rules are configured in an expert extended ACL to permit or deny some L2 packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.

- If VLAN ID-based access rules are configured in an expert extended ACL to permit or deny some L2 packets in some network segments (e.g., to prevent communication between VLAN 1 users and VLAN 2 users), ping PCs of VLAN 2 on a PC of VLAN 1. If the ping operation fails, the rules take effect.

Related Commands

Configuring an Expert Extended ACL

Command	**expert access-list extended** {*acl-name* | *acl-id* }
Parameter Description	*acl-name*: Indicates the name of an expert extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID of an expert extended ACL. If this option is configured, a numbered ACL is created. The value range of *acl-id* is 2700-2899.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an expert extended ACL and enter expert extended ACL configuration mode.

Adding ACEs to an Expert Extended ACL

Use either of the following methods to add ACEs to an expert extended ACL:

- Add ACEs in expert extended ACL configuration mode.

Command	[*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *out*: Indicates that L2 packets with the specified cos field in the outer tag are filtered. **cos inner** *in*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **VID** *out*: Indicates that L2 packets with the specified VLAN ID field in the outer tag are filtered.

	VID inner *in*: Indicates that L2 packets with the specified VLAN ID field in the inner tag are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the TOS field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Expert extended ACL configuration mode
Usage Guide	Run this command to add ACEs in expert extended ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an expert extended ACL in global configuration mode.

Command	**access-list** *acl-id* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] **[VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [{ **precedence** *precedence* | **tos** *tos* }* | **dscp** *dscp*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquelyidentifies an ACL. The value range of *acl-id* is 2700-2899. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered.

	cos *out*: Indicates that L2 packets with the specified cos field in the outer tag are filtered. **cos inner** *in*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **VID** *out*: Indicates that L2 packets with the specified VLAN ID field in the outer tag are filtered. **VID inner** *in*: Indicates that L2 packets with the specified VLAN ID field in the inner tag are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the TOS field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered expert extended ACL in global configuration mode. It cannot be used to add ACEs to a named expert extended ACL.

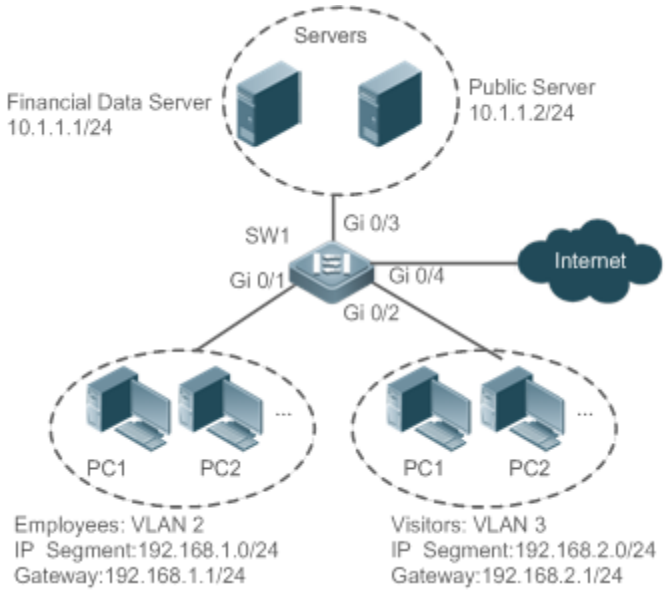
Applying an Expert Extended ACL

Command	**expert access-group** { *acl-id* **|** *acl-name* } **in**
Parameter Description	● *acl-id*: Indicates that a numbered expert extended ACL will be applied to the interface. ● *acl-name*: Indicates that a named expert extended ACL will be applied to the interface. ● **in**: Indicates that this ACL controls incoming Layer2 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an expert extended ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an Expert Extended ACL to Restrict Resources Accessible by Visitors (It is required that visitors and employees cannot communicate with each other, visitors can access the public resource server but not the financial data server of the company.)

Scenario **Figure 1-5**	
Configuration Steps	• Configure an expert extended ACL. • Add an ACE to deny packets sent from PCs in the visitor area (VLAN 3) to employee PCs in VLAN 2. • Add an ACE to prevent visitors from accessing the financial data server of the company. • Add an ACE to permit all packets. • Apply the ACL to the incoming direction of the interface of the switch that connects to the visitor area.
SW1	sw1(config)#expert access-list extended 2700 sw1(config-exp-nacl)#deny ip any any 192.168.1.0 0.0.0.255 any sw1(config-exp-nacl)#deny ip any any host 10.1.1.1 any sw1(config-exp-nacl)#permit any any any any sw1(config-exp-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
Verification	• On a visitor's PC, ping the financial data server. Verify that the ping operation fails. • On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. • On a visitor's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation

	fails. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
SW1	sw1(config)#show access-lists expert access-list extended 2700 10 deny ip any any 192.168.1.0 0.0.0.255 any 20 deny ip any any host 10.1.1.1 any 30 permit ip any any any any sw1(config)#show access-group expert access-group 2700 in Applied On interface GigabitEthernet 0/2

1.4.4 Configuring an IPv6 Extended ACL

Configuration Effect

Configure and apply an IPv6 ACL to an interface to control all incoming and outgoing IPv5 packets of this interface. You can permit or deny the entry of specific IPv6 packets to a network to control access of IPv6 users to network resources.

Configuration Steps

↘ Configuring an IPv6 ACL

- (Mandatory) Configure an IP ACL if you want to access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

↘ Adding ACEs to an IPv6 ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv6 packets of the device are denied by default.

↘ Applying an IPv6 ACL

- (Mandatory) Apply an IPv6 ACL to a specified interface on a device if you want this ACL to take effect.
- You can apply an IPv6 ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IPv6 ACL:

- Run the **ping** command to verify that the IPv6 ACL takes effect on the specified interface. For example, if an IPv6 ACL is configured to prohibit a host with a specified IP address or hosts in a specified IPv6 address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.
- Access network resources, for example, visit an IPv6 website, to check whether the IPv6 ACL takes effect on the specified interface.

Related Commands

Configuring an IPv6 ACL

Command	**ipv6 access-list** *acl-name*
Parameter Description	*acl-name*: Indicates the name of a standard or an extended IP ACL. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an IPv6 ACL and enter IPv6 configuration mode.

Adding ACEs to an IPv6 ACL

- To filter TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

Command	[*sn*] {**permit** | **deny** } *ipv6-protocol*{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* } { *destination-ipv6-prefix/prefix-length* | **any** | *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-***label flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *ipv6-protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp. *src-ipv6-prefix/prefix-len:* Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered. **host** *src-ipv6-addr*: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IPv6 packets sent from any host are filtered. *dst-ipv6-pfix/pfix-len:* Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered. **host** *dst-ipv6-addr*: Indicates that IPv6 packets sent to a host with the specified destination IP address are

	filtered. **any**: Indicates that IPv6 packets sent to any host are filtered. *op dstport*: Indicates that TCP or UDP packets are filtered based on the L4 destination port number. The value of the **op** parameter can be **eq** (equal to), **neq** (not equal to), **gt** (greater than), or **lt** (smaller than). **range** *lower upper*: Indicates that TCP or UDP packets with the L4 destination port number in the specified range are filtered. **dscp** *dscp*: Indicates that IPv6 packets with the specified the dcsp field in the header are filtered. **flow-label** *flow-label*: Indicates that IPv6 packets with the specified the flow label field in the header are filtered. **fragment:** Indicates that only fragmented IPv6 packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

- To filter IPv6 packets except for the TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

Command	[*sn*]{**permit** | **deny** } *ipv6-protocol*{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* } { *destination-ipv6-prefix/prefix-length* | **any** | *hostdestination-ipv6-address* } [**dscp** *dscp*] [**flow-***label flow-label*] [**fragment**] [**time-range** *time-range-name*] [**log**]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *ipv6-protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp. *src-ipv6-prefix/prefix-len:* Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered. **host** *src-ipv6-addr*: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IPv6 packets sent from any host are filtered. *dst-ipv6-pfix/pfix-len:* Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered.

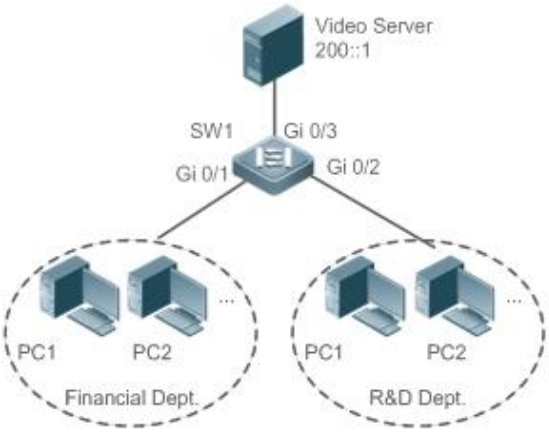
	host *dst-ipv6-addr*: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IPv6 packets sent to any host are filtered. **dscp** *dscp*: Indicates that IPv6 packets with the specified the dcsp field in the header are filtered. **flow-label** *flow-label*: Indicates that IPv6 packets with the specified the flow label field in the header are filtered. **fragment:** Indicates that only fragmented IPv6 packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

Applying an IPv6 ACL

Command	**ipv6 traffic-filter** *acl-name* **in**
Parameter Description	*acl-name*: Indicates the name of an IPv6 ACL. **in**: Indicates that this ACL controls incoming IPv6 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an IPv6 ACL take effect on the incoming or outgoing packets of the specified interface.

Configuration Example

Configuring an IPv6 ACL to Prohibit the R&D Department from Accessing the Video Server

Scenario **Figure 1-6**	
Configuration Steps	● Configure an IPv6 ACL. ● Add an ACE to the IPv6 ACL to prevent access to the video server.

	● Add an ACE to the IPv6 ACL to permit all IPv6 packets. ● Apply the IPv6 ACL to the incoming direction of the interface connected to the R&D department.
SW1	sw1(config)#ipv6 access-list dev_deny_ipv6video sw1(config-ipv6-nacl)#deny ipv6 any host 200::1 sw1(config-ipv6-nacl)#permit ipv6 any any sw1(config-ipv6-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in
Verification	● On a PC of the R&D department, ping the video server. Verify that the ping operation fails.
SW1	sw1(config)#show access-lists ipv6 access-list dev_deny_ipv6video 10 deny ipv6 any host 200::1 20 permit ipv6 any any sw1(config)#show access-group ipv6 traffic-filter dev_deny_ipv6video in Applied On interface GigabitEthernet 0/2

1.4.5 Configuring an ACL80

Configuration Effect

When the IP ACL, MAC extended ACL, expert extended ACL, and IPv6 ACL with fixed matching fields cannot meet requirements, configure the ACL80 to customize the packet fields that need to be matched.

Configuration Steps

↘ Configuring an Expert Advanced ACL

- (Mandatory) Configure an expert advanced ACL if you want to implement the ACL80 function. For details about how to configure the expert advanced ACL, see the related descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The expert advanced ACL takes effect only on the local device, and does not affect other devices on the network.

↘ Adding ACEs to an Expert Advanced ACL

- (Mandatory) Add ACEs to an expert advanced ACL to customize matching fields. If no ACE is added to the expert advanced ACL, the deny ACEs will drop all packets by default. For details about how to add an ACE to an expert advanced ACL, see the related descriptions.

Applying an Expert Advanced ACL

- (Mandatory) Apply an expert advanced ACL to a specified interface if you want this ACL take effect.
- You can apply an expert advanced ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the expert advanced ACL:
- Run the **ping** command to check whether the configurations take effect.
- Construct packets matching the ACEs to check whether ACEs take effect.

Related Commands

Configuring an Expert Advanced ACL

Command	**expert access-list advanced** *acl-name*
Parameter Description	*acl-name*: Indicates the name of an expert advanced ACL. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an expert advanced ACL and enter expert advanced ACL configuration mode.

Adding ACEs to an Expert Advanced ACL

Command	[*sn*] { **permit** | **deny** } *hex hex-mask offset*
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *hex*: Indicates the customized matching rule expressed in hexadecimal format, for example, 00d0f800. *hex-mask*: Indicates the matching mask.

	offset: Indicates the start position of matching. For example, if the matching content is 00d0f800, the matching mask is 00ff0000, and start position is 6, the destination MAC address of each packet is compared. All packets whose second byte of the destination MAC address is d0 match this ACE.
Command Mode	Expert advanced ACL configuration mode
Usage Guide	Run this command to add ACEs in expert advanced ACL configuration mode.

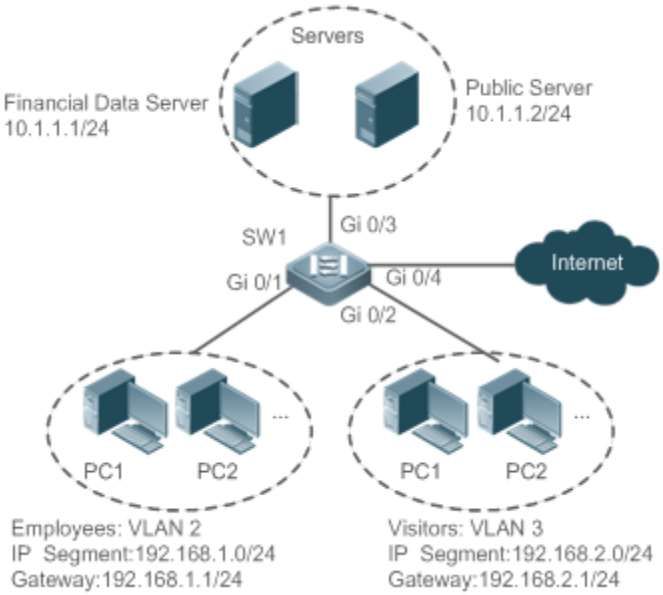
Applying an Expert Advanced ACL

Command	**expert access-group** { *acl-id* **|** *acl-name* } **in**
Parameter Description	*acl-id*: Indicates that a numbered expert advanced ACL will be applied to the interface. *acl-name*: Indicates that a named expert advanced ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming Layer2 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an expert advanced ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an ACL80 to Restrict Resources Accessible by Visitors (It is required that visitors and employees cannot communicate with each other, visitors can access the public resource server but not the financial data server of the company.)

Scenario Figure 1-7	

Configuration Steps	● Configure an expert advanced ACL. ● Add an ACE to deny packets sent from PCs in the visitor area (VLAN 3) to employee PCs in VLAN 2. ● Add an ACE to prevent visitors from accessing the financial data server of the company. ● Add an ACE to permit all packets. ● Apply the ACL to the incoming direction of the interface of the switch that connects to the visitor area.
SW1	sw1(config)#expert access-list advanced acl80-guest sw1(config-exp-dacl)#deny C0A801 FFFFFF 42 sw1(config-exp-dacl)#deny 0A010101 FFFFFFFF 42 sw1(config-exp-dacl)#permit 0806 FFFF 24 sw1(config-exp-dacl)#permit 0800 FFFF 24 sw1(config-exp-dacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#expert access-group acl80-guest in
Verification	● On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ● On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ● On a visitor's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation fails. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
SW1	sw1(config)#show access-lists expert access-list advanced sss 10 deny C0A801 FFFFFF 42 20 deny 0A010101 FFFFFFFF 42 30 permit 0806 FFFF 24 40 permit 0800 FFFF 24 expert access-group acl80-guest in Applied On interface GigabitEthernet 0/2

1.4.6 Configuring ACL Redirection

Configuration Effect

Configure the ACL redirection function on a specified interface to directly redirect specified packets on the interface to a specified port for further forwarding.

Configuration Steps

Configuring an ACL

- (Mandatory) To implement ACL redirection, you must first configure an ACL, for example, an IP, MAC extended, or expert extended ACL. For details about how to configure an ACL, see the related descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, the ACL redirection function is not available. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring ACL Redirection

- (Mandatory) Enable ACL redirection on a specified interface if you want to implement ACL redirection.
- You can configure the ACL redirection function on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

Send packets matching ACEs on the port where ACL redirection is enabled, and then use the packet capturing software on the destination port to check whether the ACL redirection function takes effect.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring ACL Redirection

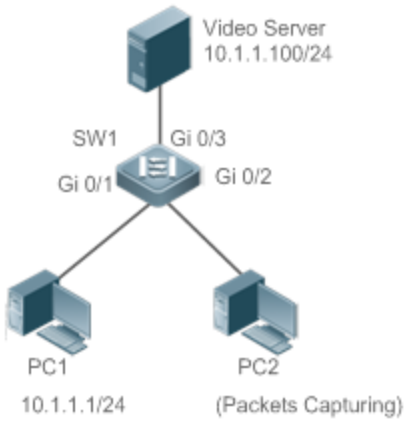
Command	**redirect destination interface** *interface-name* **acl** {*acl-id* | *acl-name* } **in**
Parameter Description	**interface** *interface-name*: Indicates the name of the destination port for redirection. *acl-id*: Indicates the ID of an ACL. *acl-name*: Indicates the name of an ACL. **in**: Indicates that incoming packets of the interface are redirected.
Command Mode	Interface configuration mode
Usage Guide	Run this command to redirect incoming packets of the interface that match ACEs to the destination port for

	further forwarding.

Configuration Example

The following configuration example describes only ACL-related configurations.

Enabling ACL Redirection to Redirect Packets Sent from the Host 10.1.1.1 to the Packet Capturing Device for Analysis

Scenario **Figure 1-8**	
Configuration Steps	● Configures an IP ACL. ● Add an ACE to the IP ACL to permit packets sent from the host 10.1.1.1. ● Enable ACL redirection on the port GI 0/1, and set the destination port to Gi 0/2.
SW1	sw1(config)#ip access-list standard 1 sw1 (config-std-nacl)#permit host 10.1.1.1 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# redirect destination interface gigabitEthernet 0/2 acl 1
Verification	● Capture packets on PC 2. Ping the video server on PC 1. Verify that ICMP requests sent from PC 1 are captured on PC 2.
SW1	sw1#show access-lists ip access-list standard 1 10 permit host 10.1.1.1 sw1#show redirect interface gigabitEthernet 0/1 acl redirect configuration on interface gigabitEthernet 0/1 redirect destination interface gigabitEthernet 0/2 acl 1 in

1.4.7 Configuring a Global Security ACL

Configuration Effect

Configure a global security ACL to prevent internal PCs of a company from accessing illegal websites or prevent virus from attacking the company's internal network. You can also configure exclusive interfaces to allow specified departments of the company to access external websites.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL if you want to protect the internal network globally. For details about the configuration method, see the earlier descriptions about the ACL.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the global security ACL does not exist. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring a Global Security ACL

- (Mandatory) Enable the global security function if you want to make the global security ACL take effect.
- You can configure a global security ACL on an access, an aggregate, or a core device based on the distribution of users.

Verification

On the internal network protected by the global security ACL, ping the website or device that are denied by ACEs to check whether the global security ACL takes effect.

Related Commands

Configuring an ACL

For details about the configuration method, see the earlier descriptions about the ACL.

Adding ACEs to an ACL

For details about the configuration method, see the earlier descriptions about the ACL.

Configuring a Global Security ACL

Command	{ **ip** | **mac** | expert } **access-group** *acl-id* **in**
Parameter Description	*acl-id*: Indicates the ID of an ACL. **in**: Filters the incoming packets of the device.

Command Mode	Global configuration mode
Usage Guide	Run this command to enable the global security ACL so that the ACL takes effect on all L2 interfaces of the device.

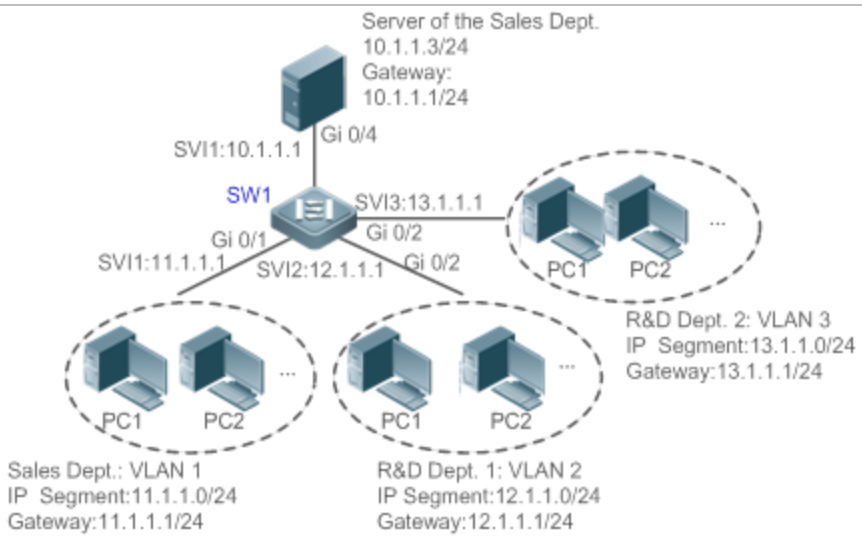
Configuring an Exclusive Interface of the Global Security ACL

Command	**no global ip access-group**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Run this command to invalidate a global security ACL on a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring a Global Security ACL to Prevent the R&D Department From Accessing the Server of the Sales Department but Allow the Sales Department to Access This Server

Scenario Figure 1-9	
Configuration Steps	● Configure an extended IP ACL "ip_ext_deny_dst_sale_server". ● Add the ACE that prevents the device to forward packets to the destination host 10.1.1.3/24. ● Configure the ACL "ip_ext_deny_dst_sale_server" as a global security ACL. ● Configure the interface directly connected to the sales department as the exclusive interface of the global security ACL.
SW1	sw1(config)#ip access-list extended ip_ext_deny_dst_sale_server

	sw1(config-ext-nacl)# deny ip any host 10.1.1.3 sw1(config-ext-nacl)#exit sw1(config)#ip access-group ip_ext_deny_dst_sale_server in sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# no global ip access-group
Verification	● On a PC of the sales department, ping the server of the sales department. Verify that the ping operation succeeds. ● On the PCs of R&D department 1 and R&D department 2, ping the server of the sales department. Verify that the ping operations fail.
	sw1#show access-lists ip access-list extended ip_ext_deny_dst_sale_server 10 deny ip any host 10.1.1.3 sw1#show running …… ! ip access-group ip_ext_deny_dst_sale_server in ! ! ! ! ! ! ! ! interface GigabitEthernet 0/1 no global ip access-group ! ……

1.4.8 Configuring a Security Channel

Configuration Effect

Configure a security channel to enable packets meeting the security channel rules to bypass the checks of access control applications. Configure the security channel if an access control application (such as DOT1X) is enabled on an uplink interface of a user, but the user should be allowed to log in to a website to download some resources (for example, downloading the SU client) before the DOT1X authentication.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured for an ACL, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring a Security Channel on a Specified Interface or Globally

- Configure a security channel on an interface if you want this security channel to take effect on the interface. Configure a global security channel if you want this security channel to take effect globally. You must configure either the interface-based security channel or the global security channel.
- You can configure a security channel on an access, an aggregate, or a core device based on the distribution of users.

Configuring an Exclusive Interface for the Global Security Channel

- (Optional) Configure an interface as the exclusive interface for the global security channel if you do not want the global security channel to take effect on this interface.

Configuring an Access Control Application

- (Optional) You can enable the DOT1X or Web authentication function to verify the security channel function.
- You can configure the access control function on an access, an aggregate, or a core device based on the distribution of users.

Verification

On a PC that is subject to the control of an access control application, ping the resources (devices or servers) that are allowed to bypass the check of the access control application to verify the configuration of the security channel.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring a Security Channel on an Interface

Command	**security access-group** {*acl-id* | *acl-name*}
Parameter Description	*acl-id*: Indicates that ID of the ACL that is configured as the security channel. *acl-name*: Indicates that name of the ACL that is configured as the security channel.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure a specified ACL as the security channel on the specified interface.

Configuring a Global Security Channel

Command	**security global access-group** {*acl-id* | *acl-name*}
Parameter Description	*acl-id*: Indicates that ID of the ACL that is configured as the security channel. *acl-name*: Indicates that name of the ACL that is configured as the security channel.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the specified ACL as the global security channel.

Configuring an Exclusive Interface for the Global Security Channel

Command	**security uplink enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the specified interface as the exclusive interface of the global security channel.

Configuration Example

The following configuration example describes only ACL-related configurations.

Enabling DOT1X Authentication and Configuring a Security Channel to Allow Users to Download the SU Software From the Server Before Authentication

Scenario **Figure 1-10**	
Configuration Steps	● Configure an expert extended ACL "exp_ext_esc". ● Add an ACE to allow forwarding packets to the destination host 10.1.1.2. ● Add an ACE to permit the DHCP packets. ● Add an ACE to permit the ARP packets. ● On the interface where DOT1X authentication is enabled, configure the ACL "exp_ext_esc" as the security channel.
SW1	sw1(config)#expert access-list extended exp_ext_esc sw1(config-exp-nacl)# permit ip any any host 10.1.1.2 any sw1(config-exp-nacl)# permit 0x0806 any any any any any sw1(config-exp-nacl)# permit tcp any any any any eq 67 sw1(config-exp-nacl)# permit tcp any any any any eq 68 sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc
Verification	● On a PC of the sales department, ping the server of the sales department. Verify that the ping operation succeeds. ● On the PCs of R&D department 1 and R&D department 2, ping the server of the sales department. Verify that the ping operations fail.
	sw1#show access-lists expert access-list extended exp_ext_esc 10 permit ip any any host 10.1.1.2 any 20 permit arp any any any any any 30 permit tcp any any any any eq 67

	40 permit tcp any any any any eq 68…… sw1#show running-config interface gigabitEthernet 0/1 Building configuration... Current configuration : 59 bytes interface GigabitEthernet 0/1 security access-group exp_ext_esc

1.4.9 Configuring the Time Range-Based ACEs

Configuration Effect

Configure the time range-based ACEs if you want some ACEs to take effect or to become invalid in a specified period of time, for example, in some time ranges during a week.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL if you want ACEs to take effect in the specified time range. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Adding an ACE with the Time Range Specified

- (Mandatory) Specify the time range when adding an ACE. For details about how to configure the time range, see the configuration manual related to the time range.

Applying an ACL

- (Mandatory) Apply the ACL to a specified interface if you want to make ACEs take effect in the specified time range.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

In the time range that the configured ACE takes effect or becomes invalid, run the **ping** command or construct packets matching the ACE to check whether the ACE takes effect or becomes invalid.

Related Commands

Configuring an ACL

For details about the ACL configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding an ACE with the Time Range Specified

For details about the ACE configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

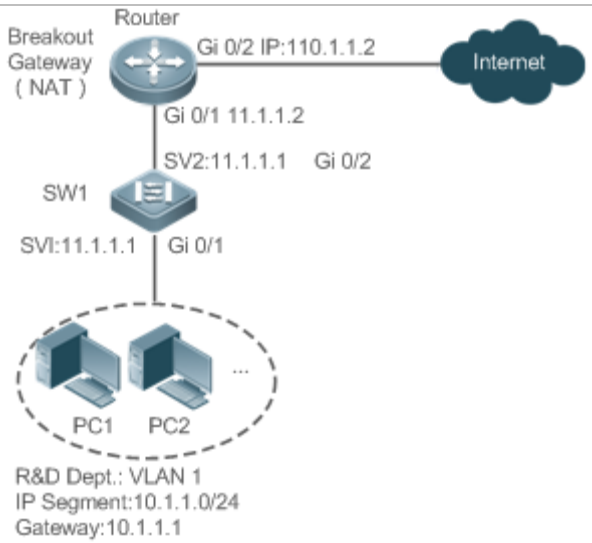
Applying an ACL

For details about the command for applying an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuration Example

The following configuration example describes only ACL-related configurations.

Adding an ACE With the Time Range Specified to Allow the R&D Department to Access the Internet Between 12:00 and 13:30 Every Day

Scenario **Figure 1-11**	
Configuration Steps	• Configure a time range named "access-internet", and add an entry of the time range between 12:00 and 13:30 every day. • Configure an IP ACL "ip_std_internet_acl". • Add an ACE to allow packets with the source IP address in the network segment 10.1.1.0/24, and associate this ACE with the time zone "access-internet". • Add an ACE to deny packets with the source IP address the network segment 10.1.1.0/24. Access to the Internet is not allowed except in the specified time range. • Add an ACE to permit all packets.

	● Apply the ACL to the inbound direction of the interface connected to the breakout gateway.
SW1	Hostname(config)# time-range access-internet Hostname(config-time-range)# periodic daily 12:00 to 13:30 Hostname(config-time-range)# exit sw1(config)# ip access-list standard ip_std_internet_acl sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255 sw1(config-std-nacl)# permit any sw1(config-std-nacl)# exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl in
Verification	● Within the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website can be opened normally. ● Beyond the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website cannot be opened.
SW1	sw1#show time-range time-range entry: access-internet (inactive) periodic Daily 12:00 to 13:30 sw1#show access-lists ip access-list standard ip_std_internet_acl 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive) 20 deny 10.1.1.0 0.0.0.255 30 permit any sw1#show access-group ip access-group ip_std_internet_acl in Applied On interface GigabitEthernet 0/2

1.4.10 Configuring Comments for ACLs

Configuration Effect

During network maintenance, if a lot of ACLs are configured without any comments, it is difficult to distinguish these ACLs later on. You can configure comments for ACLs to better understand the intended use of ACLs.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Configuring Comments for ACLs

- (Optional) Configure comments for ACLs so that it is easy to manage and understand the configured ACLs.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring Comments for ACEs

- (Optional) To facilitate understanding of a configured ACL, you can configure comments for ACEs in addition to comments for the ACL.

Verification

Run the **show access-lists** command on the device to display the comments configured for ACLs.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring a Comment for an ACL

Use either of the following two methods to configure a comment for an ACL:

Command	**list-remark** *comment*
Parameter Description	***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command	ACL configuration mode

Mode	
Usage Guide	Run this command to configure the comment for a specified ACL.

Command	**access-list** *acl-id* **list-remark** *comment*
Parameter Description	***acl-id***: Indicates the ID of an ACL. ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Configuration mode
Usage Guide	Run this command to configure the comment for a specified ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring Comments for ACEs

Use either of the following two methods to configure a comment for an ACE:

Command	**remark** *comment*
Parameter Description	***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

Command	**access-list** *acl-id* **remark** *comment*
Parameter Description	***acl-id***: Indicates the ID of an ACL. ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

1.5 Monitoring

Clearing

Description	Command
Clears the ACL packet matching counters.	**clear counters access-list** [*acl-id* | *acl-name*]
Clears the counters of packets matching the deny ACEs.	**clear access-list counters [***acl-id* |*acl-name* **]**

Displaying

Description	Command
Displays the basic ACLs.	**show access-lists** [*acl-id* | *acl-ame*] [**summary**]
Displays the redirection ACEs bound to a specified interface. If the interface is not specified, redirection ACEs bound to all interfaces are displayed.	**show redirect** [**interface** *interface-name*]
Displays the ACL configurations applied to an interface.	**show access-group** [**interface** *interface-name*]
Displays the IP ACL configurations applied to an interface.	**show ip access-group** [**interface** *interface-name*]
Displays the MAC extended ACL configurations applied to an interface.	**show mac access-group** [**interface** *interface-name*]
Displays the expert extended ACL configurations applied to an interface.	**show expert access-group** [**interface** *interface-name*]
Displays the IPv6 ACL configurations applied to an interface.	**show ipv6 traffic-filter** [**interface** *interface-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the ACL running process.	**debug acl acld event**
Debugs the ACL clients.	**debug acl acld client-show**
Debugs the ACLs created by all ACL clients.	**debug acl acld acl-show**

2 Configuring QoS

2.1 Overview

Quality of Service (QoS) indicates that a network can provide a good service capability for specified network communication by using various infrastructure technologies.

When the network bandwidth is sufficient, all data streams can be properly processed; when network congestion occurs, all data streams may be discarded. To meet users' requirements for different applications and different levels of service quality, a network must be able to allocate and schedule resources based on users' requirements and provide different levels of service quality for different data streams. To be specific, the network can process real-time and important data packets in higher priorities, and process non-real-time and common data packets in lower priorities and even discard the data packets upon network congestion.

The "doing the best" forwarding mechanism used by traditional networks cannot meet the requirements any longer and then QoS comes into being. QoS-enabled devices provide transmission QoS quality service. A transmission priority can be assigned to data streams of a type to identify the importance of the data streams. Then, the devices provide forwarding policies for different priorities, congestion mitigation and other mechanisms to provide special transmission services for these data streams. A network environment configured with QoS can provide predictability for network performance, effectively allocate network bandwidth, and reasonably utilize network resources.

2.2 Applications

Application	Description
Interface Rate Limit + Priority Relabeling	Based on different service requirements for a campus network, provide rate control and priority-based processing for outgoing traffic of the teaching building, laboratories and dormitory building.
Priority Relabeling + Queue Scheduling	Provide priority-based processing and bandwidth control for traffic of internal access to servers of an enterprise.

2.2.1 Interface Rate Limit + Priority Relabeling

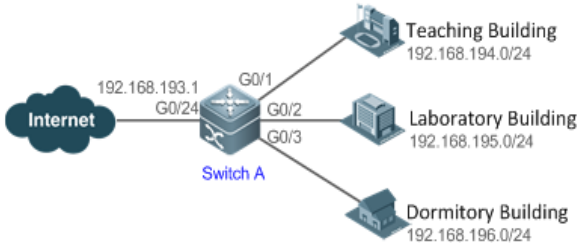
Scenario

To meet the service requirements of normal teaching, a school puts forwards the following requirements:

- Control the Internet access traffic under 100M and discard packets out of control.
- Control the outgoing traffic of the dormitory building under 50M and discard packets out of control.

- Control the rate of packets with DSCP priority 7 sent from laboratories under 20M, and change the DSCP priorities of these packets whose rates exceed 20M to 16.
- Control the outgoing traffic of the teaching building under 30M and discard packets out of control.

Figure 2-1



Remarks	A school connects GigabitEthernet 0/24 of Switch A to the Internet in the uplink and connects GigabitEthernet 0/1, GigabitEthernet 0/2 and GigabitEthernet 0/3 of Switch A to the teaching building, laboratory and dormitory building in the downlink respectively.

Deployment

- Configure the QoS interface rate limit for the interface G0/24 of Switch A for connecting the Internet.
- Configure the QoS rate limit for packets sent from the dormitory building on Switch A.
- Set the rate limit for packets with the DSCP priority 7 sent from the laboratory to 20M and relabel the DSCP priority of packets out of the rate limit to 16.
- Configure the QoS rate limit for packets sent from the teaching building on Switch A.

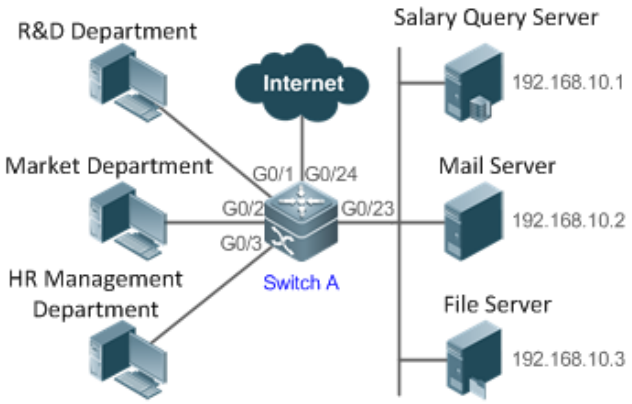
2.2.2 Priority Relabeling + Queue Scheduling

Scenario

Configure priority relabeling and queue scheduling to meet the following requirements:

- When the R&D department and market department access servers, the priorities of the server packets are as follows: mail server > file server > salary query server.
- No matter when the HR management department accesses the Internet or servers, the switch processes the corresponding packets in the highest priority.
- Since network congestion often occurs in switch running, in order to ensure smooth business operation, WRR queue scheduling must be used to schedule IP packets for 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.

Figure 2-2



Remarks	The R&D, market and HR management departments access the interfaces GigabitEthernet 0/1, GigabitEthernet 0/2 and GigabitEthernet 0/3 of Switch A respectively. The salary query server, mail server and file server are connected to GigabitEthernet 0/23 of Switch A.

Deployment

- Configure the CoS values of data streams for accessing different servers to ensure that the switch processes packets for different servers in different priorities.
- Set the default CoS value of the interface to a specific value to ensure that the switch processes packets sent by the HR management department in the highest priority.
- Configure WRR queue scheduling to ensure that data packets are transmitted in a specific quantity ratio.

2.3 Features

Basic Concept

DiffServ

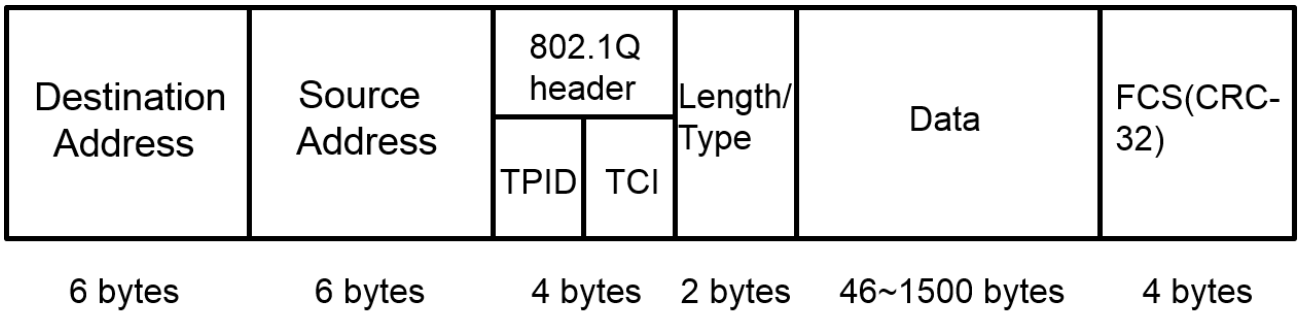
The Differentiated Services (DiffServ) Mode is an IETF system based on which QoS is implemented in Hostname products. The DiffServ system classifies all packets transmitted in a network into different types. The classification information is included in layer-2/3 packet headers, including 802.1P, IP and IP DSCP priorities.

In a DiffServ-compliant network, all devices apply the same transmission service policy to packets containing the same classification information and apply different transmission service policies to packets containing different classification information. Classification information of packets is either assigned by hosts or other devices in the network or assigned based on different application policies or different packet contents. Based on the classification information carried by packets, a device may provide different transmission priorities for different packet streams, reserve bandwidth for a kind of packet streams, discard certain packets with lower priorities, or take some other actions.

802.1P(PRI) priority

The 802.1 P priority is located at the header of a layer-2 packet with the 802.1Q header, and is used in scenarios where layer-3 headers do not need to be analyzed and QoS needs to be implemented at layer 2. Figure 2-3 shows the structure of a layer-2 packet.

Figure 2-3

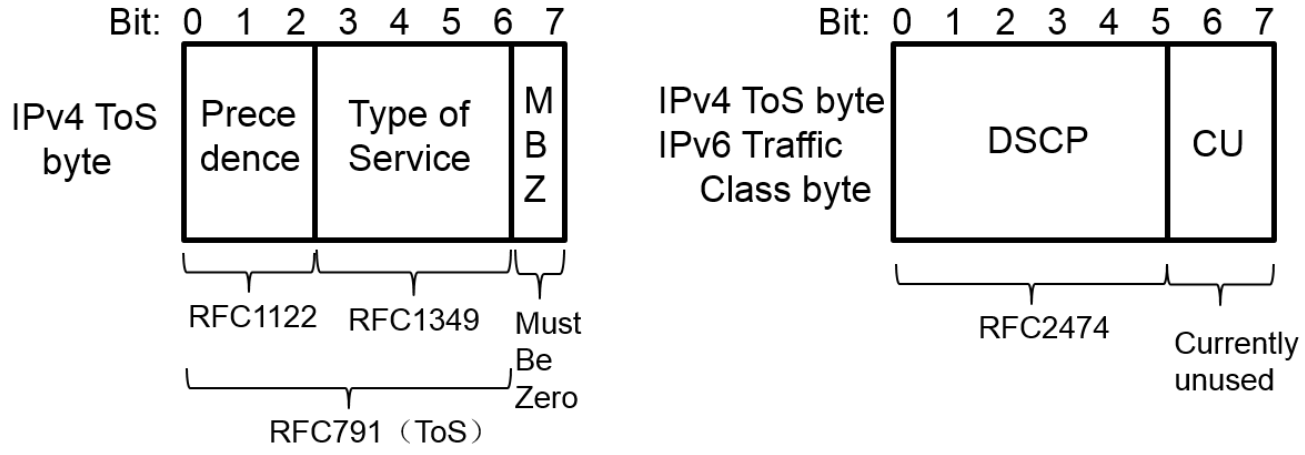


As shown in Figure 2-3, the 4-byte 802.1Q header contains 2-byte Tag ProtocolIdentifier (TPID) whose value is 0x8100 and 2-byte Tag ControlInformation (TCI). The first three bits of the TCI indicate the 802.1P priority.

IP priority (IP PRE) and DSCP priority

The priorities of IP packets are identified by the IP PRE and DSCP priority. The Type Of Service (ToS) field of the IPv4 header comprises 8 bits; where the first three bits indicate the IP precedence (IP PRE), ranging from 0 to 7. RFC 2474 redefines the ToS field of the IPv4 header, which is called the Differentiated Services (DS) field. The Differentiated Services Code Point (DSCP) priority is identified by the first 6 bits (bits 0 to 5) of the DS field, and by the first 6 bits of the Traffic Class field in the IPv6 header. Figure 2-4 shows the locations of the IP PRE and DSCP priorities in IPv4/IPv6 packets.

Figure 2-4



CoS

Class of Service (COS). The products convert packet priorities into CoS values to identity the local priorities of the packets and determine the input queue ID when packets are sent from the output interface.

Overview

Feature	Description
Stream Classification	Stream classification uses certain rules to identify packets with same characteristics and is the prerequisite and basis for distinguishing network services.
Priority Labeling and Mapping	Label packet priorities with specified values and map the values to corresponding CoS values.
Traffic Supervision	Supervise the specification of traffic flowing into a network, limit the traffic within a reasonable range, and discard the traffic out of the limit or modify the priority of the traffic.
Congestion Management	Determine the sequence of data packets sent from an interface based on the priorities of the data packets and ensure that key services can be processed in time when congestion occurs.

2.3.1 Stream Classification

Stream classification uses certain rules to identify packets with same characteristics and is the prerequisite and basis for distinguishing network services. Stream classification rules are used to distinguish different packets in the network and specify different QoS parameters for packets at different service levels.

Working Principle

Stream classification rules can be matching the PRE or DSCP priorities of IP packets or classifying packets by identifying packet content through an ACL. You can define the binding between multiple streams and stream behaviors by using commands to form policies which can be applied to interfaces for stream classification and processing.

QoS policy

A QoS policy comprises three elements: class, stream behavior and policy.

- Class

  A class identifies streams and comprises the class name and class rules. You can define the class rules by using commands to classify packets.

- Stream behavior

  Stream behaviors define the QoS actions taken for packets, including priority labeling and traffic supervision for packets.

- Policy

  A policy binds a specific class and specific stream behaviors and comprises the policy name, names of the classes bound, and stream behaviors. You can bind a specified class and stream behaviors by using a QoS policy and apply the policy to one or more interfaces.

QoS logical interface group

You can specify a series of interfaces as a QoS logical interface group (including both APs and Ethernet interfaces) and associate polices with the logical interface group for QoS processing. Take rate limit for stream behaviors for example. For packets that meet the rate limit conditions, all interfaces in the same logical interface group share the bandwidth specified by the policy.

Related Configuration

Creating a class

No class is defined by default.

You can run the **class-map** command to create a class and enter the class configuration mode.

Matching an ACL

No rules are defined for a class by default.

In the class configuration mode, you can run the **match acess-group** command to define a class rule as matching an ACL. You need to create ACL rules first.

Matching PRE priorities of IP packets

No rules are defined for a class by default.

In the class configuration mode, you can run the **match ip precedence** command to define a class rule as matching PRE priorities of IP packets. The value range of IP PRE is 0 to 7.

Matching DSCP priorities of IP packets

No rules are defined for a class by default.

In the class configuration mode, you can run the **match ip dscp** command to define a class rule as matching DSCP priorities of IP packets. The value range of DHCP priorities is 0 to 63.

Creating a policy

No policy is defined by default.

You can run the **policy-map** command to create a policy and enter the policy configuration mode.

Associating a class

A policy is not associated with any class by default.

In the policy configuration mode, you can run the **class** command to associate a class and enter the policy-class configuration mode.

Binding a stream behavior

A class is not bound to any stream behavior by default.

In the policy-class configuration mode, you can run the **set** command to modify the CoS, DSCP or VID values of a specified stream; where, the CoS value ranges from 0 to 7, the DSCP value ranges from 0 to 63 and the VID value ranges from 1 to 4094. You can run the **police** command to limit the bandwidth and process streams out of the limit for specified streams.

↘ Configuring a logical interface group

No logical interface group is defined and an interface is not added to any logical interface group by default.

In the global configuration mode, you can run the **virtual-group** command to create a logical interface group. In the interface configuration mode, you can run the **virtual-group** command to add an interface to a logical interface group. If this logical interface group is not created, you can create the logical interface group and add the interface to the group. You can create 128 logical interface groups, ranging from 1 to 128.

↘ Applying a policy to an interface

No policy is applied to an interface by default.

In the interface configuration mode, you can run the **service-policy** command to apply a policy in the input/output directions of the interface. In the global configuration mode, you can run the **service-policy** command to apply a policy in the input/output directions of all interfaces.

2.3.2 Priority Labeling and Mapping

Priorities are used to label the scheduling weights of packets or the priorities of the packets in forwarding. Different packet types have different priority types including 802.1P(PRI), IP PRE and DSCP priorities. Priority labeling and mapping refer to labeling packet priorities with specified values and mapping the values to corresponding CoS values.

Working Principle

After data streams of packets enter a device interface, the device assigns priorities to the packets based on the trust mode configured for the interface. The following describes several trust modes:

- When the interface trust mode is untrust, which means not trusting the priority information carried in packets:

  Modify the CoS value according to the default CoS value (0, which is configurable), COS-DSCP mapping table and DSCP-COS mapping table of the interface and put the packets into queues based on the final CoS value. For output packets carrying the 802.1Q tag, the packet priority will be modified to the corresponding CoS value.

- When the interface trust mode is trusting CoS:

  For packets carrying the 802.1Q tag, modify the CoS value according to the PRI value, CoS-DSCP mapping table, and DSCP-CO mapping table, and put the packets into queues based on the final CoS value. For output packets carrying the 802.1Q tag, the packet priority will be modified to the corresponding CoS value.

  For packets not carrying the 802.1Q tag, modify the CoS value according to the default CoS value (0, which is configurable), COS-DSCP mapping table and DSCP-COS mapping table of the interface, and put the packets into queues based on the final CoS value. For output packets carrying the 802.1Q tag, the packet priority will be modified to the corresponding CoS value.

- When the interface trust mode is trusting DSCP:

  For non-IP packets, the processing is the same as that for trusting CoS.

  For IP packets, modify the CoS value according to the DSCP value of the packets and the DSCP-CoS mapping table and put the packets into queues based on the final CoS value.

- When the interface trust mode is trusting IP PRE:

  For non-IPv4 packets, the processing is the same as that for trusting CoS.

  For IPv4 packets, obtain and modify the DSCP priority of the packets according to the IP PRE value of the packets and the IP-PRE-DSCP mapping table, obtain the CoS value according to the DSCP-CoS mapping table, and then put the packets into queues based on the final CoS value.

- When the trust mode and the applied policy of an interface work together:

  When the trust mode and the applied policy of an interface work together, the trust mode has a lower priority than the policy and the CoS priority can be obtained according to the DSCP-CoS mapping table.

  If a policy is applied to the interface but the policy does not has a configuration for modifying the DSCP and CoS values, the processing will be performed based on the trust mode of the interface.

Related Configuration

Configuring the trust mode of an interface

The default trust mode of an interface is untrust.

In the interface configuration mode, run the **mls qos trust** command to modify the trust mode. The trust mode can be trusting CoS, trusting DSCP or trusting IP PRE.

Configuring the default CoS value of an interface

The default CoS value of an interface is 0.

In the interface configuration mode, run the **mls qos cos** command to modify the default CoS value of the interface, which ranges from 0 to 7.

Labeling the priority of streams

The priorities of streams are not relabeled by default.

In the policy-class configuration mode, run the **set** command to modify the CoS, DSCP and VID values of streams. The CoS value ranges from 0 to 7; the DSCP value ranges from 0 to 63; the VID value ranges from 1 to 4094.

Configuring CoS-to-DSCP Map

By default, the CoS values 0, 1, 2, 3, 4, 5, 6 and 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48 and 56 respectively.

Run the **mls qos map cos-dscp** command to configure the COS-DSCP mapping. The DSCP value ranges from 0 to 63.

Configuring DSCP-to-CoS Map

By default, DSCP 0 to 7 are mapped to CoS 0, DSCP 8 to 15 mapped to CoS 1, DSCP 16 to 23 mapped to CoS2, DSCP 24 to 31 mapped to CoS 3, DSCP 32 to 39 mapped to CoS 4, DSCP 40 to 47 mapped to CoS 5, DSCP 48 to 55 mapped to CoS 6, and DSCP 56 to 63 mapped to CoS 7.

Run the **mls qos map dscp-cos** command to configure the DSCP-CoS mapping. The CoS value ranges from 0 to 7 and the DSCP value ranges from 0 to 63.

↘ Configuring IP-PRE-to-DSCP Map

By default, the IP PRE values 0, 1, 2, 3, 4, 5, 6 and 7 are mapped to the DSCP values 0, 8, 16, 24, 32, 40, 48 and 56 respectively.

Run the **mls qos map ip-prec-dscp** command to configure the IP PRE-DSCP mapping. The DSCP value ranges from 0 to 63.

2.3.3 Traffic Supervision

Supervise the specification of traffic flowing into a network, limit the traffic within a reasonable range, and discard the traffic out of the limit or modify the priority of packets. In addition, the total traffic of an interface can be monitored and the traffic out of the limit will be discarded.

Working Principle

Traffic supervision is used to monitor the specification of traffic flowing into a network and conduct preset supervision actions based on different assessment results. These actions can be:

- Forwarding: Normally forward packets within the traffic limit.
- Discarding: discard packets out of the traffic limit.
- Changing the priority and forwarding: modify the priorities of packets out of the traffic limit and then forward the packets.

Directly discard packets out of the total traffic limit of an interface.

Related Configuration

↘ Configuring the action to be conducted for traffic out of limit

No action to be conducted for traffic out of limit is configured by default.

In the policy-class configuration mode, run the **police** command to configure the action to be conducted for traffic out of limit to discarding traffic out of limit, or modifying the CoS value or DSCP value. When the traffic is out of the limit, you can modify the CoS value in the range of 0 to 7 and the DSCP value in the range of 0 to 63.

↘ Configuring the total traffic limit for an interface

The total traffic limit for an interface is not configured by default.

In the interface configuration mode, run the **rate-limit** command to configure the total traffic limit for an interface in the input and output directions.

2.3.4 Congestion Management

When the receiving rate of packets exceeds the sending rate of packets, congestion will occur on the sending interface. If no sufficient buffer is provided to store these packets, the packets may be lost. The congestion management mechanism determines the sequence of data packets to be sent from an interface based on the priorities of the data packets. The congestion management function allows for congestion control by increasing the priorities of important data packets. When

congestion occurs, the important data packets are sent in higher priorities to ensure that key services are implemented in time.

Working Principle

A queue scheduling mechanism is used for congestion management and the process is as follows:

- After each packet passes all QoS processing in a switch, the packet will obtain a CoS value finally.
- At the output interface, the device classifies the packets into corresponding sending queues based on the CoS values.
- The output interface selects packets in a queue for sending based on various scheduling policies (SP, WRR, DRR, WFQ, SP+WRR, SP+DRR and SP+WFQ).

Scheduling policy

The queue scheduling policies include SP, WRR, DRR, WFQ, SP+WRR, SP+DRR, and SP+WFQ.

- Strict-Priority (SP) scheduling means scheduling packets strictly following queue IDs. Before sending packets each time, check whether a queue with the first priority has packets to be sent. If yes, the packets in this queue are sent first. If not, check whether a queue with the second priority has packets. Follow the same rules for packets in other queues.
- Weighted Round Robin (WRR) scheduling means scheduling queues in turn to ensure that all queues have certain service time. For example, a 1000 Mbps interface has 8 output queues. The WRR configures a weighted value (5, 5, 10, 20, 20, 10, 20 and 10, which indicate the proportions of obtained resources) for each queue. This scheduling method ensures that a queue with the lowest priority is assigned with at least 50 Mbps bandwidth, which avoids that packets in the queue with the lowest priority are not served for long time when the SP scheduling method is used.
- Deficit Round Robin (DRR) scheduling is similar to the WRR, but applies weight values based on bytes, but not based on time slices.
- Weighted Fair Queueing (WFQ) scheduling provides dynamic and fair queuing and applies weighted values based on bytes, similar to the DRR. When encountering an empty queue, the DRR will shift to the next queue for transmission immediately. If a queue misses its transmission time, the queue must wait for the next time, which is the difference between the WFQ and DRR; therefore, the WFQ is more suitable for processing data packets with variable lengths than the DRR.
- SP+WRR scheduling means configuring the SP scheduling for one or more sending queues and configuring the WRR scheduling for the other queues. Among SP queues, only after all packets in the SP queue with the first priority are sent, the packets in the SP queue with the second priority can be sent. Among SP and WRR queues, only after the packets in all SP queues are sent, the packets in WRR queues can be sent.
- SP+DRR scheduling means configuring the SP scheduling for one or more sending queues and configuring the DRR scheduling for the other queues. Among SP queues, only after all packets in the SP queue with the first priority are sent, the packets in the SP queue with the second priority can be sent. Among SP and DRR queues, only after the packets in all SP queues are sent, the packets in DRR queues are sent.
- SP+WFQ scheduling means configuring the SP scheduling for one or more sending queues and configuring the WFQ scheduling for the other queues. Among SP queues, only after all packets in the SP queue with the first priority are sent,

the packets in the SP queue with the second priority can be sent. Among SP and WFQ queues, only after the packets in all SP queues are sent, the packets in WFQ queues can be sent.

Scheduling policy and round robin weight for output queues on an interface

The scheduling policies and round robin weight for output queues are based on global configurations. The device supports both global configurations and interface-based configurations. Interface-based configurations have higher priorities than global configurations. The global scheduling policy works with the corresponding global round robin weight whereas the interface scheduling policy works with the interface round robin weight. If only the global scheduling policy or interface scheduling policy is configured but no corresponding round robin weights are configured, the default round robin weights will work with the scheduling policy.

Queue bandwidth

The device allows for configuring the guaranteed minimum bandwidth and the limited maximum bandwidth for a queue. A queue configured with the guaranteed minimum bandwidth ensures that the bandwidth for this queue is not smaller than the configured value. A queue configured with the limited maximum bandwidth ensures that the bandwidth for this queue is not greater than the configured value and packets out of the bandwidth limit will be discarded.

Related Configuration

Configuring CoS-to-Queue Map

By default, the CoS values 0, 1, 2, 3, 4, 5, 6 and 7 are mapped to the queues 1, 2, 3, 4, 5, 6, 7 and 8 respectively.

Run the **priority-queue cos-map** command to configure the CoS-to-queue mapping. The CoS value ranges from 0 to 7 and the queue value ranges from 1 to 8.

Configuring the scheduling policy for an output queue

By default, the scheduling policy for a global output queue is WRR.

Run the **mls qos scheduler** command to configure the output scheduling policy for a queue. Configurable scheduling policies include SP, WRR, DRR and WFQ. You can also run the **priority-queue** command to configure the scheduling policy as SP.

Configuring the round robin weight corresponding to the WRR scheduling policy for an output queue

By default, the weight of a global queue is 1:1:1:1:1:1:1:1.

Run the **wrr-queue bandwidth** command to configure the round robin weight corresponding to the WRR scheduling policy for an output queue.

A higher weight means longer output time.

Configuring the round robin weight corresponding to the DRR scheduling policy for an output queue

By default, the weight of a global queue is 1:1:1:1:1:1:1:1.

Run the **drr-queue bandwidth** command to configure the round robin weight corresponding to the DRR scheduling policy for an output queue.

A higher weight means more packet bytes that can be sent.

Configuring the round robin weight corresponding to the WFQ scheduling policy for an output queue

By default, the weight of a global queue is 1:1:1:1:1:1:1:1.

Run the **wfq-queue bandwidth** command to configure the round robin weight corresponding to the WFQ scheduling policy for an output queue.

A higher weight means more packet bytes that can be sent.

Configuring the bandwidth for a queue

Run the **qos queue** command to configure the guaranteed minimum bandwidth and the limited maximum bandwidth for each queue. The queue value ranges from 1 to 8.

2.4 Configuration

Configuration	Description and Command	
Configuring Stream Classification	(Optional) It is used to create stream classification information.	
	class-map	Creates a class.
	match access-group	Matches ACL rules.
	match ip precedence	Matches the PRE priorities of IP packets.
	match ip dscp	Matches the DSCP priorities of IP packets.
	policy-map	Creates a policy.
	class	Associates a class.
	police	Binds the bandwidth limit for streams and the action for processing packets out of the limit.
	set	Binds the behaviors for modifying the CoS, DSCP and VID values of streams.
	virtual-group	Creates a logical interface group and adds interfaces to the logical interface group.
	service-policy	Applies a policy to an interface.
Configuring Priority Labeling and Mapping for Packets	(Optional) It is used to configure the trust mode, default CoS value and various mappings for an interface.	

Configuration	Description and Command	
	mls qos trust	Modifies the trust mode of an interface.
	mls qos cos	Modifies the default CoS value of the interface.
	mls qos map cos-dscp	Configures the CoS-to-DSCP mapping.
	mls qos map dscp-cos	Configures the DSCP-to-CoS mapping.
	mls qos map ip-precedence-dscp	Configures the IP PRE-to-DSCP mapping.
Configuring Interface Rate Limit	(Optional) It is used to configure the rate limit for an interface.	
	rate-limit	Configures the traffic limit for an interface.
Configuring Congestion Management	(Optional) It is used to configure the CoS-to-queue mapping, queue scheduling policies and round robin weight.	
	priority-queue cos-map	Configures the CoS-to-queue mapping.
	priority-queue	Configures the output scheduling policy for a queue to SP.
	mls qos scheduler	Configures the output scheduling policy for a queue.
	wrr-queue bandwidth	Configures the round robin weight corresponding to the WRR scheduling policy for an output queue.
	drr-queue bandwidth	Configures the round robin weight corresponding to the DRR scheduling policy for an output queue.
	wfq-queue bandwidth	Configures the round robin weight corresponding to the WFQ scheduling policy for an output queue.
	qos queue bandwith	Configures the guaranteed minimum bandwidth and limited maximum bandwidth for a queue.

2.4.1 Configuring Stream Classification

Configuration Effect

- Create a class and match classification rules.
- Create a policy, bind a class and stream behaviors, and associate with an interface.

Notes

- The class and policy names cannot comprise more than 31 characters.
- Interface configurations allow for only AP, SVI and Ethernet interface configurations through the **service-policy** command. When both physical interfaces and SVI interfaces are configured with policies, the priority of the physical interfaces is higher than that of the SVI interfaces.
- If run the **service-policy** command in global configuration mode, policies will be applied to all interfaces which can be configured with policies.

Configuration Steps

↘ **Creating a class and matching ACL rules**

- Optional.
- Create a class. In the class configuration mode, match ACL, IP PRE or DSCP.

↘ **Creating a policy**

- Optional.
- Create a policy. In the policy configuration mode, bind the class and stream behaviors.

↘ **Creating a logical interface group and adding interfaces to the logical interface group**

- Optional.
- Create a logical interface group and add interfaces to the logical interface group.

↘ **Applying a policy to an interface**

- Optional.
- Associate a configured policy with a specified interface or logical interface group.

Verification

- Run the **show class-map** command to check whether the class is successfully created and whether rules are successfully matched.
- Run the **show policy-map** command to check whether the policy is successfully created and whether the class and stream behaviors are successfully bound.
- Run the **show mls qos interface** command to check whether the interface is associated with the policy.

- Run the **show virtual-group** command to check the interfaces in the logical interface group.
- Run the **show mls qos virtual-group** command to check whether the logical interface group is associated with the policy.

Related Commands

Creating a class

Command	**class-map** *class-map-name*
Parameter Description	*class-map-name*: Indicates the name of a class to be created. The name cannot comprise more than 31 characters.
Command Mode	Global configuration mode
Usage Guide	-

Matching an ACL

Command	**match access-group** *access-list-number*
Parameter Description	*access-list-number*: Indicates the number of the ACL to be matched.
Command Mode	Class configuration mode
Usage Guide	-

Matching PRE of IP packets

Command	**match ip precedence** *precedence-value…* [*precedence-value…*]
Parameter Description	*precedence -value*: Indicates the IP PRE to be matched, ranging from 0 to 7.
Command Mode	Class configuration mode
Usage Guide	-

Matching DSCP of IP packets

Command	**match ip dscp** *dscp-value…* [*dscp-value…*]

Parameter Description	*dscp -value*: Indicates the DSCP to be matched, ranging from 0 to 63.
Command Mode	Class configuration mode
Usage Guide	-

Creating a policy

Command	**policy-map** *policy-map-name*
Parameter Description	*policy-map-name*: Indicates the name of a policy to be created. The name cannot comprise more than 31 characters.
Command Mode	Global configuration mode
Usage Guide	-

Associating a class

Command	**class** *class-map-name*
Parameter Description	*class-map-name*: Indicates the name of a class to be associated.
Command Mode	Policy configuration mode
Usage Guide	-

Binding the behaviors for modifying the CoS, DSCP and VID values of streams

Command	**set** { **ip dscp** *new-dscp* | **cos** *new-cos* [**none-tos**] | **vid** *new-vid* }
Parameter Description	**ip dscp** *new-dscp*: Changes the DSCP value of streams to new-dscp, ranging from 0 to 63. **cos** *new-cos*: Changes the CoS value of streams to new-cos, ranging from 0 to 7. **vid** *new-vid*: Changes the VLAN ID of streams to new-vid, ranging from 1 to 4094.
Command Mode	Class configuration mode
Usage Guide	-

Binding the bandwidth limit for streams and the action for processing packets out of the limit

Command	**police** *rate-bps burst-byte* [**exceed-action** { **drop** | **dscp** *new-dscp* | **cos** *new-cos* [**none-tos**] }]
Parameter Description	*rate-bps*: Indicates the bandwidth limit per second (KBits). The value range is from 64 to 33,554,432. *burst-byte*: Indicates the burst traffic limit (Kbytes). The value range is from 4 to 8,192. **drop**: Discards packets out of the bandwidth limit. **dscp** *new-dscp*: Changes the DSCP value of packets out of the bandwidth limit to new-dscp, ranging from 0 to 63. **cos** *new-cos*: Changes the CoS value of packets out of the bandwidth limit to new-cos, ranging from 0 to 7. **none-tos**: Does not change the DSCP value of packets when changing the CoS value of the packets.
Command Mode	Class configuration mode
Usage Guide	-

Creating a logical interface group and adding interfaces to the logical interface group

Command	**virtual-group** *virtual-group-number*
Parameter Description	*virtual-group-number*: Indicates the logical interface group number, ranging from 1 to 128.
Command Mode	Create the logical interface group in the global configuration mode, add the interface to the logical interface group in the interface configuration mode. If no logical interface group exists, you need to create a logical interface group first and then add interfaces to the logical interface group.
Usage Guide	-

Applying a policy to an interface

Command	**service-policy** { **input** | **output** } *policy-map-name*
Parameter Description	**input**: Indicates the input direction of the interface. **output**: Indicates the output direction of the interface. *policy-map-name*: Indicates the name of the policy applied to the interface.
Command Mode	Interface configuration mode/Global configuration mode
Usage Guide	-

Configuration Example

Creating four stream classes and matching ACL, IP PRE and DSCP

Configuration Steps	● Create ACL rules. ● Create four stream classes and match ACL, IP PRE and DSCP.
	`Hostname# configure terminal` `Hostname(config)# access-list 11 permit host 192.168.23.61`

	`Hostname(config)# class-map cmap1`
	`Hostname(config-cmap)# match access-group 11`
	`Hostname(config-cmap)# exit`
	`Hostname(config)# class-map cmap2`
	`Hostname(config-cmap)# match ip dscp 21`
	`Hostname(config-cmap)# exit`
	`Hostname(config)# class-map cmap3`
	`Hostname(config-cmap)# match ip precedence 5`
	`Hostname(config-cmap)# exit`

Verification	● Check whether the created ACL rules and stream class rules are successful.

	`Hostname# show access-lists`
	`ip access-list standard 11`
	`10 permit host 192.168.23.61`

	`Hostname# show class-map`
	`Class Map cmap1`
	`Match access-group 11`
	`Class Map cmap2`
	`Match ip dscp 21`
	`Class Map cmap3`
	`Match ip precedence 5`

Creating a policy, binding a class and stream behaviors, and associating with an interface

Configuration Steps	● Create the stream class cmap1, and match packets whose DSCP value is 18. Create cmap2 and match packets whose IP PRE is 7. ● Create the policy pmap1, associate the policy with cmap1, and bind the behavior of changing the CoS value of the stream to 6. Associate the policy with cmap2, bind the behavior of changing the DSCP value of the stream to 16, limiting the traffic per second within 10,000 Kbits and trigger traffic within 1024 Kbits per second, and changing the DSCP value for traffic out of limit to 7. ● Apply the policy pmap1 to the output direction of the interface gigabitEthernet 0/0. ● Create virtual logical group 1, add the interfaces gigabitEthernet 0/1 and gigabitEthernet 0/2 to the group, and apply the policy pmap1 to the input interface of the virtual logical group.
	Hostname# configure terminal Hostname(config)# class-map cmap1 Hostname(config-cmap)# match ip dscp 18 Hostname(config-cmap)# exit Hostname(config)# class-map cmap2 Hostname(config-cmap)# match ip precedence 7 Hostname(config-cmap)# exit
	Hostname(config)# policy-map pmap1 Hostname(config-pmap)# class cmap1 Hostname(config-pmap-c)# set cos 6 Hostname(config-pmap-c)# exit Hostname(config-cmap)# class cmap2 Hostname(config-pmap-c)# set ip dscp 15 Hostname(config-pmap-c)# police 10000 1024 exceed-action dscp 7 Hostname(config-pmap-c)# exit Hostname(config-pmap)# exit
	Hostname(config)# interface gigabitEthernet 0/0 Hostname(config-if-GigabitEthernet 0/0)# service-policy output pmap1 Hostname(config-if-GigabitEthernet 0/0)# exit
	Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# virtual-group 1 Hostname(config-if-GigabitEthernet 0/1)# exit

	Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-GigabitEthernet 0/2)# virtual-group 1 Hostname(config-if-GigabitEthernet 0/2)# exit Hostname(config)# virtual-group 1 Hostname(config-VirtualGroup)# service-policy input pmap1 Hostname(config-VirtualGroup)# exit
Verification	• Check whether the stream class rules are successfully created. • Check whether the policy is successfully created, and whether the stream and stream behaviors are successfully bound. • Check whether the policy is applied to the interface. • Check whether the logical interface group is successfully created, whether interfaces are successfully associated and whether the policy is successfully applied to the interface.
	Hostname# show class-map Class Map cmap1 Match ip dscp 18 Class Map cmap2 Match ip precedence 7
	Hostname# show policy-map Policy Map pmap1 Class cmap1 set cos 6 Class cmap2 set ip dscp 15 police 10000 1024 exceed-action dscp 7
	Hostname# show mls qos interface gigabitEthernet 0/0 Interface: GigabitEthernet 0/0 Ratelimit input: Ratelimit output: Attached input policy-map:

	Attached output policy-map: pmap1 Default trust: none Default cos: 0
	Hostname# show virtual-group 1 virtual-group member ---------- ---------- 1 Gi0/1 Gi0/2 Hostname# show mls qos virtual-group 1 Virtual-group: 1 Attached input policy-map: pmap1

2.4.2 Configuring Priority Labeling and Mapping for Packets

Configuration Effect

- Configure the trust mode and default CoS value of an interface.
- Configure the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings.

Notes

- Interface configurations allow for only AP and Ethernet interface configurations.

Configuration Steps

↘ **Configuring the trust mode and default CoS value of an interface**

- Optional.
- In the interface configuration mode, configure the trust mode and default CoS value of an interface.

↘ **Configuring the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings**

- Optional.
- Configure various mappings.

Verification

- Run the **show mls qos interface** command to display the trust mode and default CoS value of the interface.
- Run the **show mls qos maps** command to display the CoS-to-DSCP, DSCP-to-CoS and IP-PRE-to-DSCP mappings.

Related Commands

↘ **Configuring the trust mode of an interface**

Command	**mls qos trust** { **cos** | **ip-precedence** | **dscp** }
Parameter Description	**cos**: Configures the trust mode of an interface to CoS. **ip-precedence**: Configures the trust mode of an interface to IP PRE. **dscp**: Configures the trust mode of an interface to DSCP.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the default CoS value of an interface

Command	**mls qos cos** *default-cos*
Parameter Description	*default-cos*: Configures the default CoS value, ranging from 0 to 7. The default value is 0.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring CoS-to-DSCP MAP

Command	**mls qos map cos-dscp** *dscp1…dscp8*
Parameter Description	*dscp1….dscp8*: Indicates the DSCP values mapped to the CoS values. The default CoS values 0~7 are mapped to DSCP 0, 8, 16, 24, 32, 40, 48 and 56 respectively. The DSCP value ranges from 0 to 63.
Command Mode	Global configuration mode
Usage Guide	-

Configuring DSCP-to-CoS MAP

Command	**mls qos map dscp-cos** *dscp-list* **to** *cos*
Parameter Description	*dscp-list*: Indicates the DSCP list mapped to the CoS values. The default DSCP 0~7 are mapped to CoS 0, DSCP 8~15 mapped to CoS 1, DSCP 16~23 mapped to CoS 2, DSCP 24~31 mapped to CoS 3, DSCP 32~39 mapped to CoS 4, DSCP 40~47 mapped to CoS 5, DSCP 48~55 mapped to CoS 6, and DSCP 56~63 mapped to CoS 7. The DSCP value ranges from 0 to 63. *cos*: Indicates the CoS values mapped to the dscp-list, ranging from 0 to 7.

Command Mode	Global configuration mode
Usage Guide	-

Configuring IP-PRE-to-DSCP MAP

Command	**mls qos map ip-prec-dscp** *dscp1…dscp8*
Parameter Description	*dscp1….dscp8*: Indicates the DSCP values mapped to the IP PRE values. The default IP PRE 0~7 are mapped to DSCP 0, 8, 16, 24, 32, 40, 48 and 56 respectively. The DSCP value ranges from 0 to 63.
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

Configuring the trust mode and default CoS value of an interface

Configuration Steps	● Modify the trust mode of the interface gigabitEthernet 0/0 to DSCP. ● Change the default CoS value of the interface gigabitEthernet 0/1 to 7.
	Hostname# configure terminal Hostname(config)# interface gigabitEthernet 0/0 Hostname(config-if-GigabitEthernet 0/0)# mls qos trust dscp Hostname(config-if-GigabitEthernet 0/0)# exit Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# mls qos cos 7 Hostname(config-if-GigabitEthernet 0/1)# exit
Verification	● Check whether the trust mode and default CoS value are successfully configured for the interface.
	Hostname# show mls qos interface gigabitEthernet 0/0 Interface: GigabitEthernet 0/0 Ratelimit input: Ratelimit output:

	Attached input policy-map: Attached output policy-map: Default trust: dscp Default cos: 0 Hostname# show mls qos interface gigabitEthernet 0/1 Interface: GigabitEthernet 0/1 Ratelimit input: Ratelimit output: Attached input policy-map: Attached output policy-map: Default trust: none Default cos: 7

Configuring the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings

Configuration Steps	● Configure CoS-to-DSCP to map CoS 0, 1, 2, 3, 4, 5, 6, and 7 to DSCP 7, 14, 21, 28, 35, 42, 49, and 56 respectively. ● Configure DSCP-to-CoS to map DSCP 0, 1, 2, 3, and 4 to CoS 4 and DSCP 11, 12, 13 and 14 to CoS 7. ● Configure IP-PRE-to-DSCP to map IP PRE 0, 1, 2, 3, 4, 5, 6, and 7 to DSCP 31, 26, 21, 15, 19, 45, 47, and 61 respectively.
	Hostname# configure terminal Hostname(config)# mls qos map cos-dscp 7 14 21 28 35 42 49 56
	Hostname(config)# mls qos map dscp-cos 0 1 2 3 4 to 4 Hostname(config)# mls qos map dscp-cos 11 12 13 14 to 7
	Hostname(config)# mls qos map ip-precedence-dscp 31 26 21 15 19 45 47 61
Verification	● Check whether all mappings are successfully configured.
	Hostname# show mls qos maps cos-dscp cos dscp --- ----

```
0    7
1    14
2    21
3    28
4    35
5    42
6    49
7    56
```

```
Hostname# show mls qos maps dscp-cos
dscp cos     dscp cos     dscp cos     dscp cos
---- ---     ---- ---     ---- ---     ---- ---
 0   4        1   4        2   4        3   4
 4   4        5   0        6   0        7   0
 8   1        9   1       10   1       11   7
12   7       13   7       14   7       15   1
16   2       17   2       18   2       19   2
20   2       21   2       22   2       23   2
24   3       25   3       26   3       27   3
28   3       29   3       30   3       31   3
32   4       33   4       34   4       35   4
36   4       37   4       38   4       39   4
40   5       41   5       42   5       43   5
44   5       45   5       46   5       47   5
48   6       49   6       50   6       51   6
52   6       53   6       54   6       55   6
56   7       57   7       58   7       59   7
60   7       61   7       62   7       63   7
```

```
Hostname# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
            0 31
```

	1 26 2 21 3 15 4 19 5 45 6 47 7 61

2.4.3 Configuring Interface Rate Limit

Configuration Effect

- Configure the traffic limit for an interface.

Notes

- The configuration is supported only by Ethernet and aggregate interfaces.

Configuration Steps

Configuring the traffic limit for an interface

- Optional.
- Configure the limit on the traffic and burst traffic for an interface.

Verification

- Run the **show mls qos rate-limit** command to display the rate limit information about the interface.

Related Commands

Configuring the traffic limit for an interface

Command	**rate-limit** { **input** | **output** } *bps burst-size*
Parameter Description	**input**: Indicates the input direction of the interface. **output**: Indicates the output direction of the interface. *bps*: Indicates the bandwidth limit per second (Kbits). The value range is from 64 to 1,000,000. *burst-size*: Indicates the burst traffic limit (Kbytes). The value range is from 4 to 8,192.
Command Mode	Interface configuration mode

Usage Guide	-

Configuration Example

↘ Typical application – Interface rate limit + priority relabeling

Configuration Steps	● For Internet access by using the output interface, configure the output traffic limit on the interface G0/24, and set the bandwidth limit to 102,400 Kbits per second and burst traffic limit to 256 Kbytes per second. ● For the dormitory building, configure the input traffic limit on the interface G0/3, and set the bandwidth limit to 51,200 Kbits per second and burst traffic limit to 256 Kbytes per second. ● For the teaching building, configure the input traffic limit on the interface G0/1, and set the bandwidth limit to 30,720 Kbits per second and burst traffic limit to 256 Kbytes per second. ● For the laboratory, create the class cmap_dscp7 to match DSCP priority 7, create the policy pmap_shiyan to associate with cmap_dscp7, bind the stream behavior of changing the DSCP value for packets whose rates exceed 20M to 16, apply pmap_shiyan to the interface G0/2, and configure the interface to trusting DSCP.
	Hostname# configure terminal Hostname(config)# interface gigabitEthernet 0/24 Hostname(config-if-GigabitEthernet 0/24# rate-limit output 102400 256 Hostname(config-if-GigabitEthernet 0/24)# exit Hostname(config)# interface gigabitEthernet 0/3 Hostname(config-if-GigabitEthernet 0/3# rate-limit input 51200 256 Hostname(config-if-GigabitEthernet 0/3)# exit Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1# rate-limit input 30720 256 Hostname(config-if-GigabitEthernet 0/1)# exit
	Hostname(config)# class-map cmap_dscp7 Hostname(config-cmap)# match ip dscp 7 Hostname(config-cmap)# exit Hostname(config)# policy-map pmap_shiyan Hostname(config-pmap)# class cmap_dscp7 Hostname(config-pmap-c)# police 20480 128 exceed-action dscp 16 Hostname(config-pmap-c)# exit

	Hostname(config-pmap)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-GigabitEthernet 0/2# service-policy input pmap_shiyan Hostname(config-if-GigabitEthernet 0/2)# mls qos trust dscp Hostname(config-if-GigabitEthernet 0/2)# exit
Verification	• Check whether the interface rate limit is successfully configured. • Check whether the class and policy are successfully created and successfully applied to the interface.
	Hostname# 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
	Hostname# show class-map cmap_dscp7 Class Map cmap_dscp7 Match ip dscp 7 Hostname# show policy-map pmap_shiyan Policy Map pmap_shiyan Class cmap_dscp7 police 20480 128 exceed-action dscp 16 Hostname# 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

2.4.4 Configuring Congestion Management

Configuration Effect

- Configure the CoS-to-queue mapping.
- Configure the scheduling policy and round robin weight for an output queue.
- Configure the guaranteed minimum bandwidth and limited maximum bandwidth for a queue.

Notes

- Interface configurations allow for only AP and Ethernet interface configurations.

Configuration Steps

↘ Configuring the CoS-to-unicast mappings

- Optional.
- Configure the CoS-to-queue mappings.

↘ Configuring the scheduling policies and round robin weight for output queues

- Optional.
- Configure the scheduling policy for an output queue and modify the round robin weight.

↘ Configuring the guaranteed minimum bandwidth and limited maximum bandwidth for a queue

- Optional.
- Configure the guaranteed minimum bandwidth and limited maximum bandwidth for a queue.

Verification

- Run the **show mls qos queueing** command to display the output queue information.
- Run the **show mls qos scheduler** command to display the scheduling policy for the output queue.
- Run the **show qos bandwidth** command to display the queue bandwidth.

Related Commands

↘ Configuring CoS-to-Queue MAP

Command	**priority-queue cos-map** *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]
Parameter Description	*qid*: Indicates the queue ID to be mapped, ranging from 1 to 8. *cos0~cos7*: Indicates the CoS values to be mapped to the qid. The default CoS values 0~7 are mapped to

	queues 1~8. The value range is 0 to 7.
Command Mode	Global configuration mode
Usage Guide	-

Configuring the scheduling policy for an output queue to SP

Command	**priority-queue**
Parameter Description	**-**
Command Mode	Global configuration mode
Usage Guide	-

Configuring the scheduling policy for an output queue

Command	**mls qos scheduler** { **sp** | **wrr** | **drr** | **wfq** }
Parameter Description	**sp**: Sets the scheduling algorithm for an output queue to SP. **rr**: Sets the scheduling algorithm for an output queue to RR. **wrr**: Sets the scheduling algorithm for an output queue to WRR. **drr**: Sets the scheduling algorithm for an output queue to DRR. **wfq**: Sets the scheduling algorithm for an output queue to WFQ.
Command Mode	Global configuration mode
Usage Guide	-

Configuring the scheduling policy and round robin weight for an output queue

Command	{ **drr-queue** | **wrr-queue** | **wfq-queue** } **bandwidth** *weight1...weight8*
Parameter Description	**drr-queue**: Configures the round robin weight corresponding to the DRR scheduling policy for an output queue. **wrr-queue**: Configures the round robin weight corresponding to the WRR scheduling policy for an output queue. **wfq-queue**: Configures the round robin weight corresponding to the WFQ scheduling policy for an output

	queue. *weight1...weight8*: Indicates the weight of queues 1 to 8. The value range is from 0 to 15. The value 0 indicates that the queue uses the SP scheduling algorithm. The default weight for global/interface queues is 1:1.
Command Mode	Global/Interface configuration mode
Usage Guide	-

Configuring the guaranteed minimum bandwidth and limited maximum bandwidth for a queue

Command	**qos queue** *queue-id* **bandwidth** { **minimum** | **maximum** } *bandwidth*
Parameter Description	*queue-id*: Indicates the queue ID to be configured, ranging from 1 to 8. **minimum** *bandwidth*: Indicates the guaranteed minimum bandwidth Kbps. The value range is from 64 to 1,000,000. It is not configured by default. **maximum** *bandwidth*: Indicates the limited maximum bandwidth Kbps. The value range is from 64 to 1,000,000. It is not configured by default.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

Configuring the CoS-to-queue mapping and modifying the scheduling policy and its round robin weight

Configuration Steps	● Configure the CoS-to-queue mapping to the mapping from the CoS values 0, 1, 2, 3, 4, 5, 6, and 7 to queues 1, 2, 5, 5, 5, 5, 7, and 8. ● Configure the output scheduling policy for a queue to DRR and the round robin weight to 2:1:1:1:6:6:6:8.

	`Hostname# configure terminal`
	`Hostname(config)# priority-queue cos-map 5 2 3 4 5`
	`Hostname(config)# mls qos scheduler drr`
	`Hostname(config)# drr-queue bandwidth 2 1 1 1 6 6 6 8`

Verification	● Check whether the CoS-to-queue mapping is successfully created, and whether the output scheduling

	policy and round robin weight are successfully configured for the queue.
	Hostname# show mls qos scheduler Global Multi-Layer Switching scheduling Deficit Round Robin Hostname# show mls qos queueing CoS-to-queue map: cos qid --- --- 0 1 1 2 2 5 3 5 4 5 5 5 6 7 7 8 wrr bandwidth weights: qid weights --- ------- 1 1 2 1 3 1 4 1 5 1 6 1 7 1 8 1 drr bandwidth weights: qid weights

```
--- -------
1   2
2   1
3   1
4   1
5   6
6   6
7   6
8   8

wfq bandwidth weights:
qid weights
--- -------
1   1
2   1
3   1
4   1
5   1
6   1
7   1
8   1
```

↘ Typical application – Priority relabeling + queue scheduling

Configuration Steps	● Create ACLs for accessing various servers and create classes for matching these ACLs. ● Create policies for associating with the classes and specify new CoS values for packets accessing various servers. Associate the CoS values with the input interfaces for the R&D and market departments and configure the interfaces to trusting CoS. ● Configure the default CoS value for the HR management department interface to the highest priority 7 to ensure that packets from the HR management department are sent in the highest priority. ● Configure the output scheduling policy to WR and the round robin weight to 1:1:1:2:6:1:1:0 for the queues. This means that the SP scheduling algorithm is used for packets of the HR management department, and the packets of the R&D and market departments for accessing the mail database, file

	database and salaryquery database are scheduled based on the ratio of 6:2:1.
	Hostname# configure terminal Hostname(config)# ip access-list extended salary Hostname(config-ext-nacl)# permit ip any host 192.168.10.1 Hostname(config-ext-nacl)# exit Hostname(config)# ip access-list extended mail Hostname(config-ext-nacl)# permit ip any host 192.168.10.2 Hostname(config-ext-nacl)# exit Hostname(config)# ip access-list extended file Hostname(config-ext-nacl)# permit ip any host 192.168.10.3 Hostname(config-ext-nacl)# exit
	Hostname(config)# class-map salary Hostname(config-cmap)# match access-group salary Hostname(config-cmap)# exit Hostname(config)# class-map mail Hostname(config-cmap)# match access-group mail Hostname(config-cmap)# exit Hostname(config)# class-map file Hostname(config-cmap)# match access-group file
	Hostname(config)# policy-map toserver Hostname(config-pmap)# class mail Hostname(config-pmap-c)# set cos 4 Hostname(config-pmap-c)# exit Hostname(config-pmap)# class file Hostname(config-pmap-c)# set cos 3 Hostname(config-pmap-c)# exit Hostname(config-pmap)# class salary Hostname(config-pmap-c)# set cos 2 Hostname(config-pmap-c)# end
	Hostname(config)# interface gigabitEthernet 0/1

	Hostname(config-if-GigabitEthernet 0/1)# service-policy input toserver Hostname(config-if-GigabitEthernet 0/1)# mls qos trust cos Hostname(config-if-GigabitEthernet 0/1)# exit Hostname(config)# interface gigabitEthernet 0/2 Hostname(config-if-GigabitEthernet 0/2)# service-policy input toserver Hostname(config-if-GigabitEthernet 0/2)# mls qos trust cos Hostname(config-if-GigabitEthernet 0/2)# exit
	Hostname(config)# interface gigabitEthernet 0/3 Hostname(config-if-GigabitEthernet 0/3)# mls qos cos 7
	Hostname(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 0 Hostname(config)#mls qos scheduler wrr
Verification	● Check whether the ACLs are successfully created and whether the classes are successfully associated with the ACLs. ● Check whether the policies are successfully created, whether the classes and stream behaviors are successfully bound, and whether policies are successfully applied to the interfaces. ● Check whether the default CoS value is successfully configured for the interface and whether the scheduling policy and the round robin weight are successfully configured.
	Hostname# show access-lists ip access-list extended file 10 permit ip any host 192.168.10.3 ip access-list extended mail 10 permit ip any host 192.168.10.2 ip access-list extended salary 10 permit ip any host 192.168.10.1
	Hostname# show class-map

	Class Map salary
	  Match access-group salary
	Class Map mail
	  Match access-group mail
	Class Map file
	  Match access-group file

	Hostname# show policy-map
	
	Policy Map toserver
	  Class mail
	  set cos 4
	  Class file
	  set cos 3
	  Class salary
	  set cos 2

	Hostname# 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 Hostname# 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

	Hostname# show mls qos interface gigabitEthernet 0/3 Interface: GigabitEthernet 0/2 Ratelimit input: Ratelimit output: Attached input policy-map: Attached output policy-map: Default trust: none Default cos: 7
	Hostname# show mls qos scheduler Global Multi-Layer Switching scheduling Weighted Round Robin Hostname# Hostname#show mls qos queueing CoS-to-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
```

2.5 Monitoring

Displaying

Description	Command
Displays stream classification information.	**show class-map** [*class-map-name*]
Displays QoS policy information.	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Displays the policy applied to an interface.	**show policy-map interface** *interface-id*
Displays logical interface group information.	**show virtual-group** [*virtual-group-number* | **summary**]
Displays the policy applied to a logical interface group.	**show mls qos virtual-group** { *virtual-group-number* | **policers** }
Displays various mappings.	**show mls qos maps** { **cos-dscp** | **dscp-cos** | **ip-prec-dscp** }
Displays interface rate limit information.	**show mls qos rate-limit** [**interface** *interface-id*]
Displays the QoS queue, scheduling policy and round robin weight information.	**show mls qos queueing**
Displays the scheduling information of an output queue.	**show mls qos scheduler**
Displays the QoS information of an interface.	**show mls qos interface {** *interface-id* | **policers** }
Displays the bandwidth information of an interface.	**show qos bandwidth** [**interfaces** *interface-id*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the QoS library.	**debug qos lib** [**event** | **message**]

Debugs the QoS communication server.	**debug qos server** [**event** | **message**]
Debugs QoS user command processing.	**debug qos mls**
Debugs VMSUP configurations.	**debug qos vmsup**

Reliability Configuration

1. Configuring RLDP

1 Configuring RLDP

1.1 Overview

The Rapid Link Detection Protocol (RLDP) achieves rapid detection of unidirectional link failures, directional forwarding failures and downlink loop failures of an Ethernet. When a failure is found, relevant ports will be closed automatically according to failure treatment configuration or the user will be notified to manually close the ports to avoid wrong flow forwarding or an Ethernet layer-2 loop.

1.2 Applications

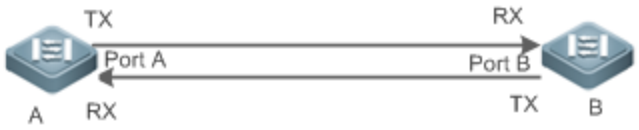
Application	Description
Unidirectional Link Detection	Detect a unidirectional link failure.
Bidirectional Forwarding Detection	Detect a bidirectional link failure.
Downlink Loop Detection	Detect a link loop.

1.2.1 Unidirectional Link Detection

Scenario

As shown in the following figure, A is connected to B via optical fiber. The two lines are the Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If any of the Tx of Port A, Rx of Port B, Tx of Port B and Rx of Port A fails, a unidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 2-1



Remarks	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.

Deployment

- Global RLDP is enabled.
- Configure unidirectional link detection under Port A and Port B and define a method for failure treatment.

1.2.2 Bidirectional Forwarding Detection

Scenario

As shown in the following figure, A is connected to B via optical fiber, and the two lines are Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If the Tx of Port A, Rx of Port B, Rx of Port A and Tx of Port B all fail, a bidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 2-2



Remarks	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.

Deployment

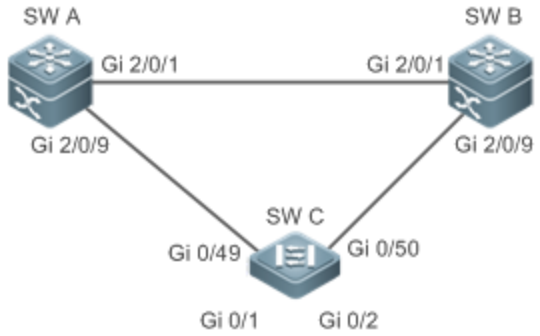
- Global RLDP is enabled.
- Configure BFD under Port A and Port B and define a method for failure treatment.

1.2.3 Downlink Loop Detection

Scenario

As shown in the following figure, A, B and C are connect into a loop. Downlink loop detection is enabled on A, and a loop is detected and treated.

Figure 2-3



Remarks	A, B and C are layer-2 or layer-3 switches. A, B and C are interconnected via exchange ports.

Deployment

- Global RLDP is enabled on A.
- Configure downlink loop detection on the Gi 2/0/1 and Gi 2/0/9 ports of A, and define a method for failure treatment.

1.3 Features

Most Ethernet link detection mechanisms detect link connectivity through automatic physical-layer negotiation. However, in some cases devices are connected on the physical layer and operate normally but layer-2 link communication is disabled or abnormal. The RLDP recognizes a neighbor device and detects a link failure through exchanging Prob packets, Echo packets or Loop packets with the device.

Basic Concepts

↘ Unidirectional Link Failure

A unidirectional link failure occurs in case of a cross-connected optical fiber, a disconnected optical fiber, an open-circuit optical fiber, one open-circuit line in a twisted-pair cable, or unidirectional open circuit of an intermediate device between two devices. In such cases, one end of a link is connected and the other disconnected so that flow is forwarded wrongly or a loop guard protocol (for example, the STP) fails.

↘ Bidirectional Link Failure

A bidirectional link failure occurs in case of two optical fibers, two open-circuit lines in a twisted-pair cable, or bidirectional open circuit of an intermediate device between two devices. In such cases, the both ends of a link are disconnected so that flow is forwarded wrongly.

↘ Loop Failure

A downlink device is wrongly connected to form a loop, resulting in a broadcast storm.

↘ RLDP Packet

The RLDP defines three types of packets: Prob packets, Echo packets and Loop packets.

- Prob packets are layer-2 multicast packets for neighbor negotiation, and unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.
- Echo packets are layer-2 unicast packets as response to Prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.
- Loop packets are layer-2 multicast packets for downlink loop detection. They can only be received. The default encapsulation format is SNAP.

RLDP Detection Interval and Maximum Detection Times

A detection interval and the maximum detection times can be configured for the RLDP. A detection interval determines the period of sending Prob packets and Loop packets. When a device receives a Prob packet, it replies with an Echo packet immediately. A detection interval and the maximum detection times determine the maximum detection time (equal to a detection interval × the maximum detection times + 1) for unidirectional or bidirectional link detection. If neither Prob nor Echo packet from a neighbor can be received within the maximum detection time, the treatment of unidirectional or bidirectional failure will be triggered.

RLDP Neighbor Negotiation

When configured with unidirectional or bidirectional link detection, a port can learn a peer-end device as its neighbor. One port may learn one neighbor, which is variable. If negotiation is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation, which succeeds when a port receives a Prob packet from the neighbor. However, if the RLDP is enabled under a failure, the port cannot learn a neighbor so that detection cannot start. In this case, recover the link state before enabling the RLDP.

Treatment for Failed Port under RLDP

- Warning: Only print Syslog to indicate a failed port and a failure type.
- Shutdown SVI: Print Syslog, and then inquire an SVI according to the Access VLAN or Native VLAN of a port and shut down the SVI if the port is a physical exchange port or layer-2 AP member port.
- Port violation: Print Syslog, and configure a failed port as in violation state, and the port will enter Linkdown state physically.
- Block: Print Syslog, and configure the forward state of a port as Block, and the port will not forward packets.

Recovery of Failed Port under RLDP

- Manual reset: Manually reset all failed ports to initialized state and restart link detection.
- Manual or automatic errdisable recovery: Recover all failed ports to initialized state manually or regularly (30s by default and configurable) and restart link detection.
- Automatic recovery: Under unidirectional or bidirectional link detection, if the treatment for failed ports is not specified as port violation, recover ports to initialized state based on Prob packets and restart link detection.

Port State under RLDP

- normal: Indicates the state of a port after link detection is enabled.
- error: Indicates the state of a port after a unidirectional or bidirectional link failure or a loop failure is detected.

Overview

Feature	Description

Deploying RLDP Detection	Enable unidirectional or bidirectional link detection or downlink loop detection for failures and implement treatment.

1.3.1 Deploying RLDP Detection

The RLDP provides unidirectional link detection, bidirectional forwarding detection and downlink loop detection.

Working Principle

Unidirectional Link Detection

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives Prob packets but no Echo packets, or none of them, treatment for a unidirectional failure will be triggered and detection will stop.

Bidirectional Forwarding Detection

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives neither Prob packets nor Echo packets from a neighbor, treatment for a bidirectional failure will be triggered and detection will stop.

Downlink Loop Detection

When this function is enabled, a port sends Loop packets regularly. In the following cases, a loop failure will be triggered after the same port or a different port receives the packets: in one case, the egress and ingress ports are the same routed port or layer-3 AP member port; in another case, the egress and ingress ports are exchange ports or layer-2 AP member ports in a same default VLAN and in Forward state. Treatment for the failure will be implemented and detection will stop.

Related Configuration

- Configuring RLDP Detection

By default, RLDP detection is disabled.

You may run the global command **rldp enable** or the interface command **rldp port** to enable RLDP detection and specify a detection type and treatment.

You may run the **rldp neighbor-negotiation** command to specify neighbor negotiation, the **rldp detect-interval** command to specify a detection interval, the **rldp detect-max** command to specify the number of detection times, the **rldp error-recover interval** command to specify the interval for periodically recovering a failed port, or the **rldp reset** command to recover a failed port.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic RLDP Functions	(Mandatory) It is used to enable RLDP detection in global configuration mode.	
	rldp enable	Enables global RLDP detection on all ports.
	(Mandatory)It is used to specify a detection type in interface configuration mode and failure treatment for an interface.	
	rldp port	Enables RLDP detection on a port and specifies a detection type and failure treatment.
	(Optional)It is used to configure a detection interval, detection times and neighbor negotiation in global configuration mode.	
	rldp detect-interval	Modifies global RLDP parameters on all ports, such as the detection interval, maximum detection times and neighbor negotiation.
	rldp detect-max	
	rldp neighbor-negotiation	
	rldp error-recover interval	Specifies the interval for the RLDP to periodically recover a failed port.
	(Optional) It is used in privileged EXEC mode.	
	rldp reset	Recovers all ports.

1.4.1 Configuring Basic RLDP Functions

Configuration Effect

- Enable RLDP unidirectional link detection, bidirectional forwarding detection, downlink loop detection, or VLAN-based loop detection to discover loop failures.

Notes

- Loop detection is effective to all member ports of an AP when configured on one of the ports. Unidirectional link detection and bidirectional forwarding detection are effective only on an AP member port.
- The loop detection on a physical port added to an AP shall be configured the same as that of the other member ports. There are three cases. First, if loop detection is not configured on a newly-added port but on the existing member ports, the new port adopts the configuration and detection results of the existing ports. Second, if a newly-added port and the existing member ports have different loop detection configuration, the new port adopts the configuration and detection results of the existing ports.

- When configuring the RLDP on an AP port, you may configure failure treatment only as "shutdown-port", to which other configurations will be modified.
- When "shutdown-port" is configured on a port, RLDP detection cannot be restored in case of a failure. After troubleshooting, you may run the **rldp reset** or **errdisable recovery** command to restore the port and resume detection. For configuration of the **errdisable recovery** command, please refer to the *Configuring Interface*.
- The VLAN-based loop detection function (configured by the **rldp port vlan-loop-detec** command) can be configured only on multi-VLAN ports such as trunk and hybrid ports. It is recommended not to configure this function on access or routed ports. This function does not take effect when configured on routed ports.
- It is recommended not to configure the **rldp port vlan-loop-detect** command and the **rldp port loop-detect** command on the same port. The **rldp port loop-detect** command is mainly configured on access ports to detect downlink loops.
- The VLAN list for the VLAN-based loop detection function needs to be configured in consideration of performance, and should include only VLANs that possibly encounter loops to reduce invalid detection and improve detection performance.
- The VLAN-based loop detection function can be configured only on AP member ports. It is recommended to configure the same detection VLAN on all member ports of an AP to ensure normal loop detection.

Configuration Steps

Enabling RLDP

- Mandatory.
- Enable RLDP detection on all ports in global configuration mode.

Enabling Neighbor Negotiation

- Optional.
- Enable the function in global configuration mode, and port detection will be started under successful neighbor negotiation.

Configuring Detection Interval

- Optional.
- Specify a detection interval in global configuration mode.

Configuring Maximum Detection Times

- Optional.
- Specify the maximum detection times in global configuration mode.

Configuring the Interval to Periodically Recover a Failed Port

- Optional.

- Configure the interval for periodic recovery in global configuration mode.

Configuring Detection under Port

- Mandatory.
- Configure unidirectional RLDP detection, bidirectional RLDP detection or downlink loop detection in interface configuration mode, and specify failure treatment.

Restoring All Failed Ports

- Optional.
- Enable this function in privileged mode to restore all failed ports and resume detection.

Verification

- Display the information of global RLDP, port and neighbor.

Related Commands

Enabling Global RLDP Detection

Command	**rldp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable global RLDP detection.

Enabling RLDP Detection on Interface

Command	**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }** **rldp port vlan-loop-detect { warning | isolate-vlan} vlan** *vlan-list*
Parameter Description	**unidirection-detect**: Indicates unidirectional link detection. **bidirection-detect**: Indicates bidirectional forwarding detection. **loop-detect**: Indicates downlink loop detection. **vlan-loop-detect**: Indicates VLAN-based loop detection. **warning**: Indicate the failure treatment is warning. **shutdown-svi**: Indicate the failure treatment is closing the SVI that the interface is on. **shutdown-port**: Indicates the failure treatment is port violation. **block**: Indicates the failure treatment is disabling learning and forwarding of a port. **isolate-vlan**: Indicates that the failure treatment is isolation for the faulty VLAN. **vlan-list**: Indicates the VLANs to be detected.

Command Mode	Interface configuration mode
Usage Guide	The interfaces include layer-2 switch ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports.

Modifying Global RLDP Detection Parameters

Command	**rldp** {**detect-interval** *interval* | **detect-max** *num* | **neighbor-negotiation** }
Parameter Description	**detect-interval** *interval*: Indicates a detection interval. **detect-max** *num*: Indicates detection times. **neighbor-negotiation**: Indicates neighbor negotiation.
Command Mode	Global configuration mode
Usage Guide	Modify all RLDP parameters on all ports when necessary.

Recovering Failed Port

Command	**rldp reset**
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	Recover all failed ports to initialized state and resume detection.

Displaying RLDP State Information

Command	**show rldp** [**interface** *interface-name*]
Parameter Description	*interface-name*: Indicates the interface to display information of.
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	Display RLDP state information.

Configuration Example

Enabling RLDP Detection in Ring Topology

Scenario **Figure 2-4**	As shown in the following figure, the aggregation and access sections are in a ring topology. The STP is enabled on all devices to prevent loop and provide redundancy protection. To avoid a unidirectional or bidirectional link failure resulting in STP failure, RLDP unidirectional and bidirectional link detection is enabled between aggregation devices as well as between an aggregation device and the access device. To avoid loop due to wrong downlink connection of the aggregation devices, enable RLDP downlink loop detection on the downlink ports of the aggregation devices and of the access device. To avoid loop due to wrong downlink connection of the access device, enable RLDP downlink loop detection on the downlink

	ports of the access device. 
Configuration Steps	● SW A and SW B are aggregation devices, and SW C is an access device. Users connected to SW C. SW A, SW B and SW C are structured in a ring topology, and the STP is enabled on each of them. For STP configuration, refer to relevant configuration guide. ● Enable the RLDP on SW A, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port. ● Enable the RLDP on SW B, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port. ● Enable the RLDP on SW C, enable unidirectional and bidirectional link detection on the two uplink ports, and enable loop detection on the two downlink ports.

A	`A#configure terminal`
	`A(config)#rldp enable`
	`A(config)#interface GigabitEthernet 2/0/1`
	`A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port`
	`A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port`
	`A(config-if-GigabitEthernet 2/0/1)# exit`
	`A(config)#interface GigabitEthernet 2/0/9`
	`A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port`
	`A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port`
	`A(config-if-GigabitEthernet 2/0/1)#rldp port loop-detect shutdown-port`
	`A(config-if-GigabitEthernet 2/0/1)#exit`

B	`Apply the configuration on SW A.`

C	`C#configure terminal`
	`C(config)#rldp enable`
	`C(config)#interface GigabitEthernet 0/49`

	C(config-if-GigabitEthernet 0/49)#rldp port unidirection-detect shutdown-port C(config-if-GigabitEthernet 0/49)#rldp port bidirection-detect shutdown-port C(config-if-GigabitEthernet 0/49)# exit C(config)#interface GigabitEthernet 0/50 C(config-if-GigabitEthernet 0/50)#rldp port unidirection-detect shutdown-port C(config-if-GigabitEthernet 0/50)#rldp port bidirection-detect shutdown-port C(config-if-GigabitEthernet 0/50)#exit C(config)#interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port C(config-if-GigabitEthernet 0/1)#exit C(config)#interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port C(config-if-GigabitEthernet 0/2)#exit
Verification	● Check the RLDP information on SW A, SW B and SW C. Take SW A for example.
A	A#show rldp rldp state : enable rldp hello interval: 3 rldp max hello : 2 rldp local bridge : 00d0.f822.33aa ---------- Interface GigabitEthernet 2/0/1 port state : normal neighbor bridge : 00d0.f800.51b1 neighbor port : GigabitEthernet 2/0/1 unidirection detect information: action: shutdown-port state : normal bidirection detect information: action: shutdown-port state : normal Interface GigabitEthernet 2/0/9

	port state : normal neighbor bridge : 00d0.f800.41b0 neighbor port : GigabitEthernet 0/49 unidirection detect information: action: shutdown-port state : normal bidirection detect information: action: shutdown-port state : normal loop detect information: action: shutdown-port state : normal

Common Errors

- RLDP functions and private multicast address authentication or TPP are enabled at the same time.
- Neighbor negotiation is not enabled when configuring unidirectional or bidirectional link detection. The RLDP should be enabled on a neighbor device, or otherwise a unidirectional or bidirectional failure will be detected.
- If RLDP detection is configured to be implemented after neighbor negotiation while configuring unidirectional or bidirectional link detection, detection cannot be implemented as no neighbor can be learned due to a link failure. In this situation, you are suggested to recover the link state first.
- You are suggested not to specify the failure treatment as Shutdown SVI under a routed port.
- You are suggested not to specify the failure treatment as Block for a port, on which a loop protection protocol is enabled, for example, the STP.

Common Errors

- When the **exec-cmd** command is executed for interface configuration, the input of the corresponding AP wired port is incorrect.
- When the RLDP loop detection configurations are modified, the **no exec-cmd** command is not executed to delete the original configurations or the **exec-cmd** command is not re-executed to cancel the configurations.

1.5 Monitoring

Displaying

Description	Command
Displays RLDP state.	**show rldp** [**interface** *interface-name*]

Network Management & Monitoring Configuration

1. Configuring SNMP
2. Configuring NTP
3. Configuring SPAN and RSPAN
4. Configuring sFlow

1 Configuring SNMP

1.1 Overview

Simple Network Management Protocol (SNMP) became a network management standard RFC1157 in August 1988. At present, because many vendors support SNMP, SNMP has in fact become a network management standard and is applicable to the environment where systems of multiple vendors are interconnected. By using SNMP, the network administrator can implement basic functions such as information query for network nodes, network configuration, fault locating, capacity planning, and network monitoring and management.

↘ SNMP Versions

Currently, the following SNMP versions are supported:

- SNMPv1: The first official version of SNMP, which is defined in RFC1157.
- SNMPv2C: Community-based SNMPv2 management architecture, which is defined in RFC1901.
- SNMPv3: SNMPv3 provides the following security features by identifying and encrypting data.

1. Ensuring that data is not tampered during transmission.
2. Ensuring that data is transmitted from legal data sources.
3. Encrypting packets and ensuring data confidentiality.

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 Applications

Application	Description
Managing Network Devices Based on SNMP	Network devices are managed and monitored based on SNMP.

1.2.1 Managing Network Devices Based on SNMP

Scenario

Take the following figure as an example. Network device A is managed and monitored based on SNMP network manager.

Figure 1-1



Remarks	A is a network device that needs to be managed. PC is a network management station.

Deployment

The network management station is connected to the managed network devices. On the network management s tation, users access the Management Information Base (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.

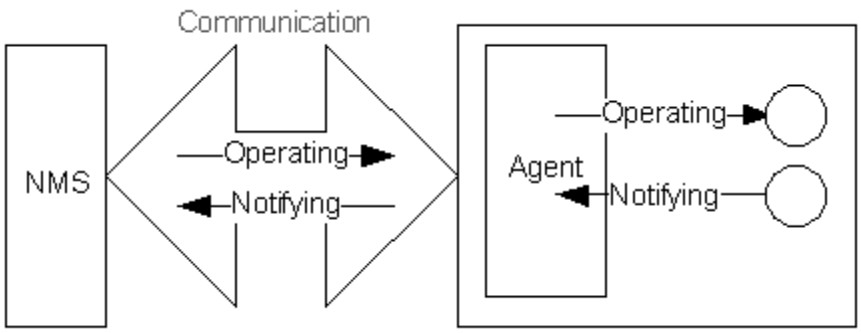
1.3 Features

Basic Concepts

SNMP is an application layer protocol that works in C/S mode. It consists of three parts:

- SNMP network manager
- SNMP agent
- MIB

Figure 1-2 shows the relationship between the network management system (NMS) and the network management agent.



SNMP Network Manager

The SNMP network manager is a system that controls and monitors the network based on SNMP and is also called the NMS.

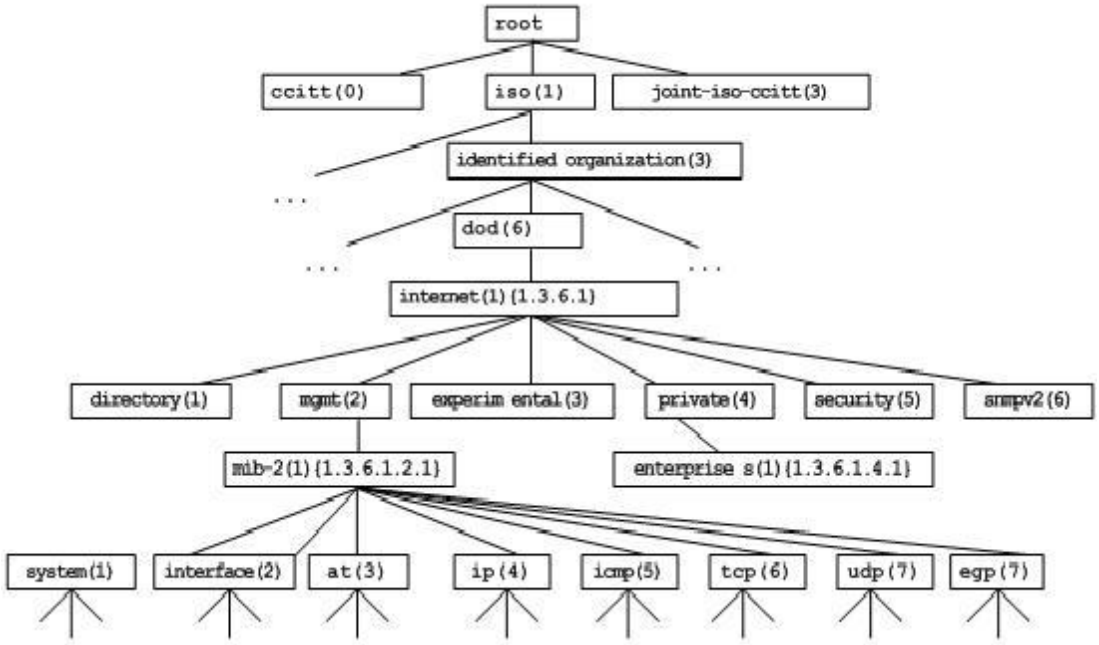
SNMP Agent

The SNMP agent (hereinafter referred to as the 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 may be used to uniquely identify a management unit system among network devices. The MIB is a collection of unit identifiers of network devices.

Figure 1-3 Tree Hierarchical Structure



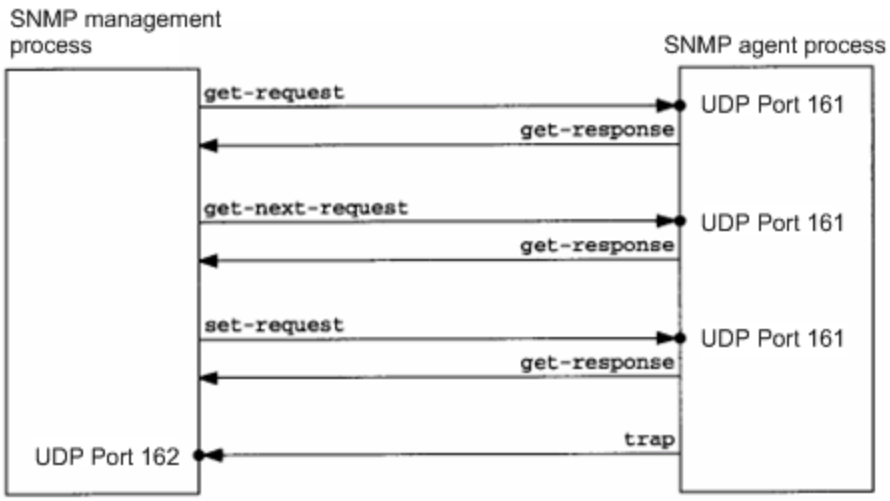
Operation Types

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 in response to the three operations performed by the agent on the NMS.
- Trap: The agent actively sends a message to notify the NMS of something that happens.

The first four packets are sent by the NMS to the agent and the last two packets are sent by the agent to the NMS. (Note: SNMPv1 does not support the Get-bulk operation.) Figure 1-4 describes the operations.

Figure 1-4 SNMP Packet Types



The three operations performed by the NMS on the agent 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.

Overview

Feature	Description
Basic SNMP Functions	The SNMP agent is configured on network devices to implement basic functions such as information query for network nodes, network configuration, fault locating, and capacity planning.
SNMPv1 and SNMPv2C	SNMPv1 and SNMPv2C adopt the community-based security architecture, including authentication name and access permission.
SNMPv3	SNMPv3 redefines the SNMP architecture, namely, it enhances security functions, including the security model based on users and access control model based on views. The SNMPv3 architecture already includes all functions of SNMPv1 and SNMPv2C.

1.3.1 Basic SNMP Functions

Working Principle

Working Process

SNMP protocol interaction is response interaction (for exchange of packets, see Figure 1-4). 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.

Related Configuration

Shielding or Disabling the SNMP Agent

By default, the SNMP function is enabled.

The **no snmp-server** command is used to disable the SNMP agent.

The **no enable service snmp-agent** command is used to directly disable all SNMP services.

Setting Basic SNMP Parameters

By default, the system contact mode, system location, and device Network Element (NE) information are empty. The default serial number is 60FF60, the default maximum packet length is 1,572 bytes, and the default UDP port ID of the SNMP service is 161.

The **snmp-server contact** command is used to configure or delete the system contact mode.

The **snmp-server location** command is used to configure or delete the system location.

The **snmp-server chassis-id** command is used to configure the system serial number or restore the default value.

The **snmp-server packetsize** command is used to configure the maximum packet length of the agent or restore the default value.

The **snmp-server net-id** command is used to configure or delete the device NE information.

The **snmp-server udp-port** command is used to set the UDP port ID of the SNMP service or restore the default value.

Configuring the SNMP Host Address

By default, no SNMP host is configured.

The **snmp-server host** command is used to configure the NMS host address to which the agent actively sends messages or to delete the specified SNMP host address. In the messages sent to the host, the SNMP version, receiving port, authentication name, or user can be bound. This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

Setting Trap Message Parameters

By default, SNMP is not allowed to actively send a trap message to the NMS, the function of sending a Link Trap message on an interface is enabled, the function of sending a system reboot trap message is disabled, and a trap message does not carry any private field.

By default, the IP address of the interface where SNMP packets are sent is used as the source address.

By default, the length of a trap message queue is 10 and the interval for sending a trap message is 30s.

The **snmp-server enable traps** command is used to enable or disable the agent to actively send a trap message to the NMS.

The **snmp trap link-status** command is used to enable or disable the function of sending a Link Trap message on an interface.

The **snmp-server trap-source** command is used to specify the source address for sending messages or to restore the default value.

The **snmp-server queue-length** command is used to set the length of a trap message queue or to restore the default value.

The **snmp-server trap-timeout** command is used to set the interval for sending a trap message or to restore the default value.

The **snmp-server trap-format private** command is used to set or disable the function of carrying private fields in a trap message when the message is sent.

The **snmp-server system-shutdown** command is used to enable or disable the function of sending a system reboot trap message.

↘ Setting the SNMP Attack Protection and Detection Function

By default, the SNMP attack protection and detection function is disabled.

The **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** } command is used to set and enable the attack protection and detection function.

1.3.2 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).

Working Principle

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. The authentication name of the NMS must be the same as an authentication name defined in devices.

SNMPv2C adds the Get-bulk operation mechanism and can return more detailed error message types to the management workstation. The Get-bulk operation is performed to obtain all information from a table or obtain lots of data at a time, so as to reduce the number of request responses. 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 errors. Now, errors can be differentiated based on error codes. Because management workstations supporting SNMPv1 and SNMPv2C may exist on the

network, the SNMP agent must be able to identify SNMPv1 and SNMPv2C packets and return packets of the corresponding versions.

Security

One authentication name has the following attributes:

- Read-only: Provides the read permission of all MIB variables for authorized management workstations.
- Read-write: Provide the read/write permission of all MIB variables for authorized management workstations.

Related Configuration

Setting Authentication Names and Access Permissions

The default access permission of all authentication names is read-only.

The **snmp-server community** command is used to configure or delete an authentication name and access permission.

This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed.

1.3.3 SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2 into the SNMPv3 system.

Working Principle

The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications of SNMP, which work by using the services provided by the SNMP engine.

SNMPv3v determines whether a user has the right to use MIB objects by using the User-based Security Model (USM). The security level of the NMS user must be the same as that of an SNMP user defined in devices so as to manage devices.

SNMPv3 requires the NMS to obtain the SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the discover and report operation mechanisms. When the NMS does not know agent engine IDs, 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.

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.

SNMPv1 and SNMPv2C Security Models and Security Levels

Security Model	Security Level	Authentication	Encryption	Description

SNMPv1	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.
SNMPv2c	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.

SNMPv3 Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User name.	N/A	Data validity is confirmed through user name.
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 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, one SNMP engine uniquely identifies an SNMP entity in a management domain. Therefore, the SNMPv3 agent as an entity must has a unique engine ID, that is, SnmpEngineID.

An engine ID is an octet string that consists of 5 to 32 bytes. RFC3411 defines the format of an engine ID:

- The first four bytes indicate the private enterprise ID (allocated by 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 27 bytes, which is defined by the vendor.
- 5: Hexadecimal value consisting of 27 bytes, which is defined by the vendor.
- 6-127: Reserved.
- 128-255: Formats specified by the vendor.

Related Configuration

Configuring an MIB View and a Group

By default, one view is configured and all MIB objects can be accessed.

By default, no user group is configured.

The **snmp-server view** command is used to configure or delete a view and the **snmp-server group** command is used to configure or delete a user group.

One or more instructions can be configured to specify different community names so that network devices can be managed by NMSs of different permissions.

Configuring an SNMP User

By default, no user is configured.

The **snmp-server user** command is used to configure or delete a user.

The NMS can communicate with the agent by using only legal users.

An SNMPv3 user can specify the security level (whether authentication and encryption are required), authentication algorithm (MD5 or SHA), authentication password, encryption password (only DES is available currently), and encryption password.

1.3.4 The Trap Record Function

If the connection between the NMS and the device is interrupted, the NMS will lose the trap alarm information during the disconnection. After the NMS is reconnected, the trap alarm record function supports the NMS in collecting the alarms of the device through SNMP (for details, see relevant documents of ARALM-MIB.mib), to fill in the missing trap alarm information during the disconnection.

Related Configuration

Configuring the SNMP Traps with Device Serial Numbers

Run the **snmp-server trap-format device-serial-number** command to configure the SNMP traps with device serial numbers.

Configuring the SNMP Traps with Sysmacs

Run the **snmp-server trap-format sysmac** command to configure the SNMP traps with sysmacs.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic SNMP Functions	(Mandatory) It is used to enable users to access the agent through the NMS.	
	enable service snmp-agent	Enables the agent function.
	snmp-server community	Sets an authentication name and access permission.
	snmp-server user	Configures an SNMP user.
	snmp-server view	Configures an SNMP view.
	snmp-server group	Configures an SNMP user group.
	snmp-server authentication	Configures the SNMP attack protection and detection function.

Configuration	Description and Command	
Enabling the Trap Function	(Optional) It is used to enable the agent to actively send a trap message to the NMS.	
	snmp-server host	Configures the NMS host address.
	snmp-server enable traps	Enables the agent to actively send a trap message to the NMS.
	snmp trap link-status	Enables the function of sending a Link Trap message on an interface.
	snmp-server system-shutdown	Enables the function of sending a system reboot trap message.
	snmp-server trap-source	Specifies the source address for sending a trap message.
	snmp-server trap-format private	Enables a trap message to carry private fields when the message is sent.
Shielding the Agent Function	(Optional) It is used to shield the agent function when the agent service is not required.	
	no snmp-server	Shields the agent function.
Setting SNMP Control Parameters	(Optional) It is used to set or modify SNMP control parameters.	
	snmp-server contact	Sets the device contact mode.
	snmp-server location	Sets the device location.
	snmp-server logging	Sets the logging function.
	snmp-server chassis-id	Sets the serial number of the device.
	snmp-server net-id	Sets NE information about the device.
	snmp-server packetsize	Modifies the maximum packet length.
	snmp-server udp-port	Modifies the UDP port ID of the SNMP service.
	snmp-server queue-length	Modifies the length of a trap message queue.
	snmp-server trap-timeout	Modifies the interval for sending a trap message.
	(Optional) It is used to configure the trap record function.	
	snmp-server trap-format device-serial-number	Configures the SNMP traps with device serial numbers.
	snmp-server trap-format sysmac	Configures the SNMP traps with sysmacs.

1.4.1 Configuring Basic SNMP Functions

Configuration Effect

Enable users to access the agent through the NMS.

Notes

- By default, no authentication name is set on network devices and SNMPv1 or SNMPv2C cannot be used to access the MIB of network devices. When an authentication name is set, if no access permission is specified, the default access permission is read-only.

Configuration Steps

Configuring an SNMP View

- Optional
- An SNMP view needs to be configured when the View-based Access Control Model (VACM) is used.

Configuring an SNMP User Group

- Optional
- An SNMP user group needs to be configured when the VACM is used.

Configuring an Authentication Name and Access Permission

- Mandatory
- An authentication name must be set on the agent when SNMPv1 and SNMPv2C are used to manage network devices.

Configuring an SNMP User

- Mandatory
- A user must be set when SNMPv3 is used to manage network devices.

Enabling the Agent Function

- Optional
- By default, the agent function is enabled. When the agent function needs to be enabled again after it is disabled, this command must be used.

Enabling the SNMP Attack Protection and Detection Function

- Optional
- By default, the SNMP attack protection and detection function is disabled. When malicious attacks need to be prevented, the configuration item must be used on the agent.

Configuring the Password Dictionary Checking for Communities and Users

- Optional
- By default, the password dictionary checking for communities and users is not configured.

Verification

Run the **show snmp** command to check the SNMP function on devices.

Related Commands

Configuring an SNMP View

Command	**snmp-server view** *view-name oid-tree* { **include** | **exclude** }
Parameter Description	*view-name*: View name *oid-tree*: MIB objects associated with a view, which are displayed as an MIB subtree. **include:** Indicates that the MIB object subtree is included in the view. **exclude:** Indicates that the MIB object subtree is not included in the view.
Command Mode	Global configuration mode
Usage Guide	Specify a view name and use it for view-based management.

Configuring an SNMP User Group

Command	**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]
Parameter Description	**v1** | **v2c** |**v3:** Specifies the SNMP version. **auth:** Messages sent by users in the group need to be verified but data confidentiality is not required. This configuration is valid for SNMPv3 only. **noauth:** Messages sent by users in the group do not need to be verified and data confidentiality is not required. This configuration is valid for SNMPv3 only. **priv:** Messages sent by users in the group need to be verified and confidentiality of transmitted data is required. This configuration is valid for SNMPv3 only. *readview*: Associates one read-only view. *writeview*: Associates one read/write view. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-adname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Associate certain users with a group and associate the group with a view. Users in a 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.

Configuring an Authentication Name and Access Permission

Command	**snmp-server community** [*0* | *7*] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]
Parameter Description	*0*: Indicates that the input community string is a plaintext string. *7*: Indicates that the input community string is a ciphertext string.

	string: Community string, which is equivalent to the communication password between the NMS and the SNMP agent. *view-name*: Specifies a view name for view-based management. **ro:** Indicates that the NMS can only read variables of the MIB. **rw:** The NMS can read and write variables of the MIB. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified. *ipaddr*: Associates NMS addresses and specifies NMS addresses for accessing the MIB.
Command Mode	Global configuration mode
Usage Guide	This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed. To disable the SNMP agent function, run the **no snmp-server** command.

Configuring an SNMP User

Command	**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]
Parameter Description	*username*: User name. *groupname*: Specifies the group name for a user. **v1** | **v2c** | **v3:** Specifies the SNMP version. Only SNMPv3 supports later security parameters. **encrypted:** The specified password input mode is ciphertext input. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 protocol authentication key consists of 16 bytes and an SHA authentication protocol key consists of 20 bytes. Two characters stand for one byte. Encrypted keys are valid for this engine only. **auth:** Specifies whether authentication is used. **md5:** Specifies the MD5 authentication protocol. **sha** specifies the SHA authentication protocol. *auth-password*: Configures a password string (not more than 32 characters) used by the authentication protocol. The system converts the passwords into the corresponding authentication keys. **priv:** Specifies whether confidentiality is used. **des56** specifies the use of the 56-bit DES encryption protocol. *priv-password*: Configures a password string (not more than 32 characters) used for encryption. The system converts the password into the corresponding encryption key. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-adname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from

	which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Configure user information so that the NMS can communicate with the agent by using a valid user. For an SNMPv3 user, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (at present, only DES is available), and encryption password.

Enabling the Agent Function

Command	**enable service snmp-agent**
Parameter Description	
Configuration mode	Privileged mode.
Usage Guide	This command is used to enable the SNMP agent function of a device.

Enabling the SNMP Attack Protection and Detection Function

Command	**snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }
Parameter Description	*times*: Number of continuous failed attempts. **lock:** After continuous authentication fails, the source IP address is permanently forbidden to initiate authentication for access. The administrator needs to manually unlock the IP address. **lock-time** *minutes*: After continuous authentication fails, the source IP address is forbidden to initiate authentication for access in a period of time. Beyond the period, the source IP address can be authenticated for access again. **unlock:** After continuous authentication fails, the source IP address is allowed to access the MIB continuously, which is equivalent to the fact that the SNMP attack protection and detection function is not configured.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP attack protection and detection function so that the corresponding measure can be taken after continuous authentication fails. The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses. The source IP address that are forbidden to access the MIB in a period of time can be authenticated for access again after the period expires or after the administrator manually unlocks the IP addresses.

Displaying the SNMP Status Information

Command	**show snmp** [**mib** | **user** | **view** | **group| host | process-mib-time**]
Parameter Description	**mib:** Displays information about the SNMP MIB supported in the system. **user:** Displays information about an SNMP user.

	view: Displays information about an SNMP view. **group:** Displays information about an SNMP user group. **host:** Displays information about user configuration. **process-mib-time:** Displays the MIB node with the longest processing time.
Configuration mode	Privileged mode.
Usage Guide	N/A

Configuring the Password Dictionary Checking for Communities and Users

Command	**snmp-server enable secret-dictionary-check**
Parameter Description	N/A
Configuration mode	Global configuration mode.
Usage Guide	This command must be used together with the **password policy** command in the global configuration mode.

Configuration Example

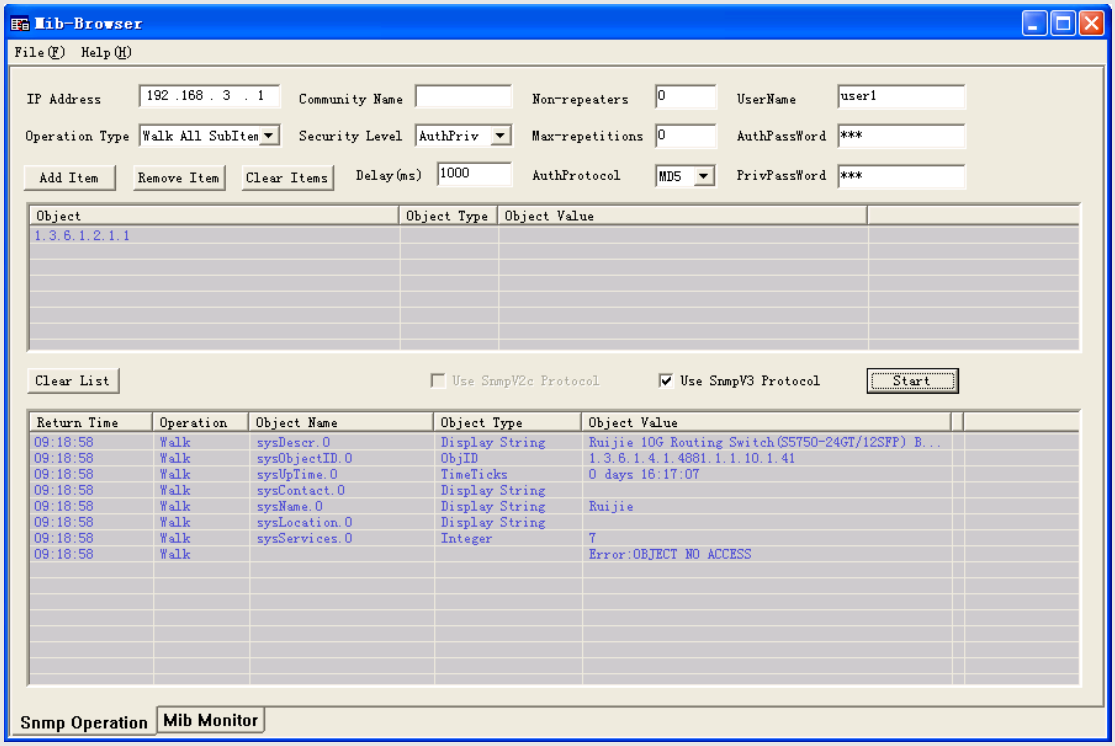
Configuring SNMPv3 Configuration (Specified View)

Scenario Figure 1-5	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● Network devices can control the operation permission of users to access MIB objects. For example, the user named user1 can read MIB objects under the system node (1.3.6.1.2.1.1) and can only write MIB objects under the SysContact node (1.3.6.1.2.1.1.4.0). ● Network devices can actively send authentication and encryption messages to the NMS.
Configuration Steps	● Configure a MIB view and a MIB group. Create a MIB view “view1”, which includes the associated MIB object (1.3.6.1.2.1.1); then create a MIB view “view2”, which includes the associated MIB object

	(1.3.6.1.2.1.1.4.0). Create a group “g1”, select the version “v3”, set the security level to the authentication and encryption mode “priv”, and configure permissions to read the view “view1” and write the view “view2”. ● Configure an SNMP user. Create a user named “user1” under group “g1”, select “v3” as the version, and set the authentication mode to “md5”, authentication password to “123”, encryption mode to “DES56”, and encryption password to “321”. ● Configure the SNMP host address. Set the host address to 192.168.3.2, select “3” as the version, set the security level to the authentication and encryption mode “priv”, and associate the user name “user1”. Enable the agent to actively send a trap message to the NMS. ● Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	Hostname(config)#snmp-server view view1 1.3.6.1.2.1.1 include Hostname(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include Hostname(config)#snmp-server group g1 v3 priv read view1 write view2 Hostname(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 Hostname(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 Hostname(config)#snmp-server enable traps Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 Hostname(config-if-gigabitEthernet 0/1)#exit
Verification	1. Run the **show running-config** command to display configuration information of the device. 2. Run the **show snmp user** command to display the SNMP user. 3. Run the **show snmp view** command to display the SNMP view. 4. Run the **show snmp group** command to display the SNMP group. 5. Run the **show snmp host** command to display the host information configured by the user. 6. Install MIB-Browser.
Agent	Hostname# show running-config ! interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 ! snmp-server view view1 1.3.6.1.2.1.1 include snmp-server view view2 1.3.6.1.2.1.1.4.0 include snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56

	D5CEC4884360373ABBF30AB170E42D03 snmp-server group g1 v3 priv read view1 write view2 snmp-server host 192.168.3.2 traps version 3 priv user1 snmp-server enable traps
	Hostname# show snmp user User name: user1 Engine ID: 800013110300d0f8221120 storage-type: permanent active Security level: auth priv Auth protocol: MD5 Priv protocol: DES Group-name: g1
	Hostname#show snmp view view1(include) 1.3.6.1.2.1.1 view2(include) 1.3.6.1.2.1.1.4.0 default(include) 1.3.6.1
	Hostname# show snmp group groupname: g1 securityModel: v3 securityLevel:authPriv readview: view1 writeview: view2 notifyview:
	Hostname#show snmp host Notification host: 192.168.3.2 udp-port: 162 type: trap user: user1 security model: v3 authPriv
	Install MIB-Browser, enter IP address 192.168.3.1 in **IP Address** and **user1** in **UserName**, select **AuthPriv** for **Security Level**, enter **123** in **AuthPassWord**, select **MD5** for **AuthProtocol**, and enter **321**

in **PrivPassWord**. Click **Add Item** and select a management unit for which the MIB needs to be queried, for example, **System** in the following figure. Click **Start**. The MIB is queried for network devices. The lowest pane in the following figure shows query results.



Common Errors

-

1.4.2 Enabling the Trap Function

Configuration Effect

Enable the agent to actively send a trap message to the NMS.

Notes

N/A

Configuration Steps

Configuring the SNMP Host Address

- Optional
- Configure the host address of the NMS when the agent is required to actively send messages.

Enabling the Agent to Actively Send a Trap Message to the NMS

- Optional

- Configure this item on the agent when the agent is required to actively send a trap message to the NMS.

Enabling the Function of Sending a Link Trap Message on an Interface

- Optional
- Configure this item on the agent when a link trap message needs to be sent on an interface.

Enabling the Function of Sending a System Reboot Trap Message

- Optional
- Configure this item on the agent when the system is required to send a trap message to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

- Optional
- Configure this item on the agent when it is required to permanently use a local IP address as the source SNMP address to facilitate management.

Enabling a Trap Message to Carry Private Fields when the Message Is Sent

- Optional
- Configure this item on the agent when private fields need to be carried in a trap message.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Setting the NMS Host Address

Command	**snmp-server host**{ *host-addr* | **ipv6** *ipv6-addr* } [**traps | inrorms**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]
Parameter Description	*host-addr*: Address of the SNMP host. *ipv6-addr*: (IPv6) address of the SNMP host. **traps | informs:** Configures the host to send a trap message or an inform message. **version:** SNMP version, which can be set to **V1**, **V2C**, or **V3**. **auth** | **noauth** | **priv:** Sets the security level of V3 users. *community-string*: Community string or user name (V3). *port-num*: Configures the port ID of the SNMP host. *notification-type*: Type of trap messages that are actively sent, for example, snmp. If no trap type is specified, all trap messages are sent.
Command	Global configuration mode

Mode	
Usage Guide	This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

Enabling the Agent to Actively Send a Trap Message to the NMS

Command	**snmp-server enable traps** [*notification-type*]
Parameter Description	*notification-type*: Enables trap notification for the corresponding events, including the following types: snmp: Enables trap notification for SNMP events. bridge: Enables trap notification for bridge events. mac-notification: Enables trap notification for MAC events. ospf: Enables trap notification for OSPF events. vrrp: Enables trap notification for VRRP events. web-auth: Enables trap notification for Web authentication events.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **snmp-server host** command to so that trap messages can be actively sent.

Enabling the Function of Sending a Link Trap Message on an Interface

Command	**snmp trap link-status**
Parameter Description	**-**
Configuration mode	Interface configuration mode
Usage Guide	For interfaces (Ethernet interface, AP interface, and SVI interface), when this function is enabled, the SNMP sends a Link Trap message if the link status on the interfaces changes. Otherwise, the SNMP does not send the message.

Enabling the Function of Sending a System Reboot Trap Message

Command	**snmp-server system-shutdown**
Parameter Description	-
Configuration mode	Global configuration mode
Usage Guide	When the function of notification upon SNMP system reboot is enabled, a trap message is sent to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

Command	**snmp-server trap-source** *interface*
Parameter Description	*interface*: Used as the interface for the SNMP source address.

Configuration mode	Global configuration mode
Usage Guide	By default, the IP address of the interface where SNMP packets are sent is used as the source address. To facilitate management and identification, this command can be run to permanently use one local IP address as the source SNMP address.

Enabling a Trap message to Carry Private Fields when the Message Is Sent

Command	**snmp-server trap-format private**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to enable a trap message to carry private fields when the message is sent. At present, supported private fields include the alarm generation time. For the specific data types and data ranges of the fields, see TRAP-FORMAT-MIB.mib.

Configuration Example

Enabling the Trap Function

Scenario Figure 1-6	 ● The NMS manages network devices (agents) based on the community authentication mode, and network devices can actively send messages to the NMS.
Configuration Steps	1. Perform configuration to enable the agent to actively send messages to the NMS. Set the SNMP host address to 192.168.3.2, the message format to Version2c, and the authentication name to user1. Enable the agent to actively send trap messages. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.

Agent	`Hostname(config)#snmp-server host 192.168.3.2 traps version 2c user1`
	`Hostname(config)#snmp-server enable traps`
	`Hostname(config)#interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0`
	`Hostname(config-if-gigabitEthernet 0/1)#exit`

Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp** command to display the SNMP status.

Agent	Hostname# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location fuzhou snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact ruijie.com.cn snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	Hostname#show snmp Chassis: 1234567890 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs

	0 Trap PDUs SNMP global trap: enabled SNMP logging: disabled SNMP agent: enabled

Common Errors

N/A

1.4.3 Shielding the Agent Function

Configuration Effect

Shield the agent function when the agent service is not required.

Notes

- Run the **no snmp-server** command to shield the SNMP agent function when the agent service is not required.
- Different from the shielding command, after the **no enable service snmp-agent** command is run, all SNMP services are directly disabled (that is, the SNMP agent function is disabled, no packet is received, and no response packet or trap packet is sent), but configuration information of the agent is not shielded.

Configuration Steps

Shielding the SNMP Agent Function for the Device

- Optional
- To shield the configuration of all SNMP agent services, use this configuration.

Disabling the SNMP Agent Function for the Device

- Optional
- To directly disable all services, use this configuration.

Verification

Run the **show services** command to check whether SNMP services are enabled or disabled.

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Shielding the SNMP Agent Function for the Device

Command	**no snmp-server**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	By default, the SNMP agent function is disabled. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are set, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must also be run at the same time 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. Run the **no snmp-server** command to disable SNMP agent services of all versions supported by the device. After this command is run, all SNMP agent service configurations are shielded (that is, after the **show running-config** command is run, no configuration is displayed. Configurations are restored after the SNMP agent service is enabled again). After the **enable service snmp-agent** command is run, the SNMP agent configurations are not shielded.

Disabling the SNMP Agent Function for the Device

Command	**no enable service snmp-agent**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to disable the SNMP service, but it will not shield SNMP agent parameters.

Configuration Example

Enabling the SNMP Service

Scenario Figure 1-7	 After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.
Configuration Steps	1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	`Hostname(config)#enable service snmp-agent`
Verification	1. Run the **show services** command to check whether the SNMP service is enabled or disabled.
Agent	`Hostname#show service`

	web-server : disabled web-server(https): disabled snmp-agent : enabled ssh-server : disabled telnet-server : enabled

Common Errors

N/A

1.4.4 Setting SNMP Control Parameters

Configuration Effect

Set basic parameters of the SNMP agent, including the device contact mode, device location, serial number, and parameters for sending a trap message. By accessing the parameters, the NMS can obtain the contact person of the device and physical location of the device.

Notes

N/A

Configuration Steps

Setting the System Contact Mode

- Optional
- When the contact mode of the system needs to be modified, configure this item on the agent.

Setting the System Location

- Optional
- When the system location needs to be modified, configure this item on the agent.

Setting the System Serial Number

- Optional
- When the system serial number needs to be modified, configure this item on the agent.

Setting NE Information about the Device

- Optional
- When the NE code needs to be modified, configure this item on the agent.

Setting the Maximum Packet Length of the SNMP Agent

- Optional

- When the maximum packet length of the SNMP agent needs to be modified, configure this item on the agent.

Setting the UDP Port ID of the SNMP Service

- Optional
- When the UDP port ID of the SNMP service needs to be modified, configure this item on the agent.

Setting the Queue Length of Trap Messages

- Optional
- When the size of the message queue needs to be adjusted to control the message sending speed, configure this item on the agent.

Setting the Interval for Sending a Trap Message

- Optional
- When the interval for sending a trap message needs to be modified, configure this item on the agent.

Configuring SNMP Flow Control

- Optional
- If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Enabling the Functions of SNMP Versions

- Optional
- Configure this command in the agent if the SNMP version needs modification.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Setting the System Contact Mode

Command	**snmp-server contact** *text*
Parameter Description	*text*: String that describes the system contact mode.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting the System Location

Command	**snmp-server location** *text*
Parameter Description	*text*: String that describes system information.
Configuration mode	Global configuration mode
Usage Guide	N/A

Setting the System Serial Number

Command	**snmp-server chassis-id** *text*
Parameter Description	*text*: Text of the system serial number, which maybe digits or characters.
Configuration mode	Global configuration mode
Usage Guide	In general, the device serial number is used as the SNMP serial number to facilitate identification of the device.

Setting NE Information about the Device

Command	**snmp-server net-id** *text*
Parameter Description	*text*: Text that is used to set the device NE code. The text is a string that consists of 1 to 255 characters that are case-sensitive and mayinclude spaces.
Configuration mode	Global mode.
Usage Guide	Set the NE code of the device.

Setting the Maximum Packet Length of the SNMP Agent

Command	**snmp-server packetsize** *byte-count*
Parameter Description	*byte-count*: Packet size, ranging from 484 bytes to 17,876 bytes.
Configuration mode	Global mode.
Usage Guide	N/A

Setting the UDP Port ID of the SNMP Service

Command	**snmp-server udp-port** *port-num*
Parameter Description	*port-num*: Specifies the UDP port ID of the SNMP service, that is, the ID of the protocol port that receives SNMP packets.
Configuration mode	Global mode.
Usage Guide	Specify the protocol port ID for receiving SNMP packets.

Setting the Length of a Trap Message Queue

Command	**snmp-server queue-length** *length*
Parameter Description	*length*: Queue length, ranging from 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the size of the message queue to control the message sending speed.

Setting the Interval for Sending a Trap Message

Command	**snmp-server trap-timeout** *seconds*
Parameter Description	*seconds*: Interval (unit: second). The value range is 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

Configuring SNMP Flow Control

Command	**snmp-server flow-control pps** [*count*]
Parameter Description	*count*: Number of SNMP request packets processed per second. The value range is 50 to 65,535.
Command Mode	Global configuration mode
Usage Guide	If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Enabling the Functions of SNMP Versions

Command	**snmp-server version** { **v1** | **v2c** | **v3** }
Parameter Description	v1: SNMPv1 v2: SNMPv2c v3: SNMPv3
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Setting SNMP Control Parameters

Scenario **Figure 1-8**	 ● The NMS manages network devices (agents) based on the community authentication mode and can obtain basic system information about the devices, for example, system contact mode, location, and serial number.
Configuration Steps	1. Set SNMP agent parameters. Set the system location, contact mode, and serial number. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.

Agent	`Hostname(config)#snmp-server location fuzhou`
	`Hostname(config)#snmp-server contact ruijie.com.cn`
	`Hostname(config)#snmp-server chassis-id 1234567890`
	`Hostname(config)#interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0`
	`Hostname(config-if-gigabitEthernet 0/1)#exit`

Verification	1. Check the configuration information of the device. 2. Check the SNMP view and group information.

Agent	`Hostname# show running-config`
	`ip access-list standard a1`
	`10 permit host 192.168.3.2`
	`interface gigabitEthernet 0/1`
	`no ip proxy-arp`
	`ip address 192.168.3.1 255.255.255.0`
	`snmp-server view v1 1.3.6.1.2.1.1 include`
	`snmp-server location fuzhou`
	`snmp-server host 192.168.3.2 traps version 2c user1`
	`snmp-server enable traps`
	`snmp-server contact ruijie.com.cn`
	`snmp-server community user1 view v1 rw a1`
	`snmp-server chassis-id 1234567890`

	Hostname#show snmp view v1(include) 1.3.6.1.2.1.1 default(include) 1.3.6.1 Hostname#show snmp group groupname: user1 securityModel: v1 securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview: groupname: user1 securityModel: v2c securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview:

1.4.5 Configuring the Trap Record Function

Configuration Effect

Configure the trap record function to obtain all historical trap information of a device.

Related Commands

Configuring the SNMP Traps with Device Serial Numbers

Command	**snmp-server trap-format device-serial-number**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the SNMP Traps with Sysmacs

Command	**snmp-server trap-format sysmac**
Parameter Description	N/A

Configuration mode	Global configuration mode
Usage Guide	N/A

1.5 Monitoring

Clearing

Description	Command
Clears the list of source IP addresses that are locked after continuous authentication fails.	**clear snmp locked-ip** [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Displaying

Description	Command
Displays the SNMP status.	**show snmp** [**mib** | **user** | **view** | **group**| **host** | **locked-ip** | **process-mib-time**]

2 Configuring NTP

2.1 Overview

The 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.

Currently, devices can be used both as NTP clients and NTP servers. In other words, a device can synchronize time with a time server, and be used 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.

Protocols and Standards

- RFC 1305 : Network Time Protocol (Version 3)

2.2 Applications

Application	Description
Synchronizing Time Based on an External Reference Clock Source	A device is used as a client that synchronizes time with an external clock source. After successful synchronization, it is used as a server to provide time synchronization for other devices.
Synchronizing Time Based on a Local Reference Clock Source	A device uses a local clock as a reliable NTP reference clock source and is also used as a server to provide time synchronization for other devices.

2.2.1 Synchronizing Time Based on an External Reference Clock Source

Scenario

As shown in Figure 3-1:

- DEVICE-A is used as a reliable reference clock source to provide time synchronization for external devices.
- DEVICE-B specifies DEVICE-A as the NTP server and synchronizes time with DEVICE-A.
- After successful synchronization, DEVICE-B provides time synchronization for DEVICE-C.

Figure 3-1



Deployment

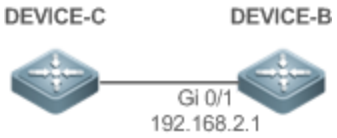
Configure DEVICE-B to the NTP external reference clock mode.

2.2.2 Synchronizing Time Based on a Local Reference Clock Source

Scenario

As shown in Figure 3-2, DEVICE-B uses a local clock as the NTP reference clock source and provides time synchronization for DEVICE-C.

Figure 3-2



Deployment

Configure DEVICE-B to the NTP local reference clock mode.

2.3 Features

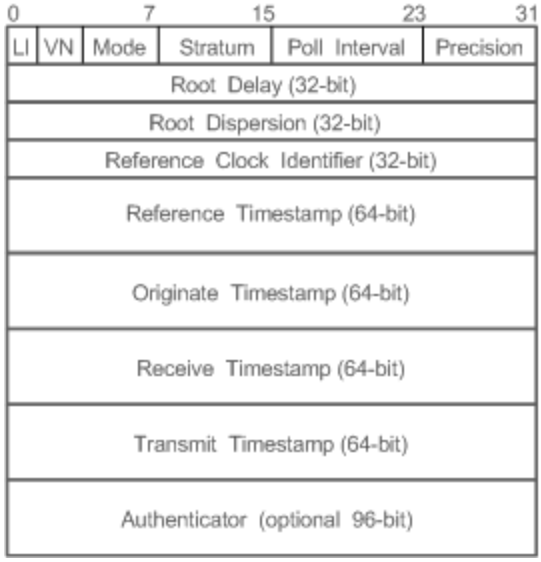
Basic Concepts

NTP Packet

As defined in RFC1305, NTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 3-3 shows the format of an NTP time synchronization packet.

Figure 3-3 Format of an NTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP version number. The current version number is 3.
- Mode: indicates a 3-bit NTP working mode.

0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master reference clock source; other values: indicate slave reference clock sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master reference clock source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

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 is used as an NTP client that synchronizes time with an NTP server in the network.

Stratum

In NTP, "stratum" is used to describe the hops from a device to an authority clock source. An NTP server whose stratum is 1 has a directly connected atomic clock or radio controlled clock; an NTP server whose stratum is 2 obtains time from the server whose stratum is 1; an NTP server whose stratum is 3 obtains time from the server whose stratum is 2; and so on. Therefore, clock sources with lower stratums have higher clock precisions.

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.

Overview

Feature	Description
NTP Time Synchronization	Network devices synchronize time with their servers or reliable clock sources to implement high-precision time correction.
NTP Security Authentication	The NTP packet encryption authentication is used to prevent unreliable clock sources from time synchronization interference on a device.
NTP Access Control	An Access Control List (ACL) is used to filter sources of received NTP packets.

2.3.1 NTP Time Synchronization

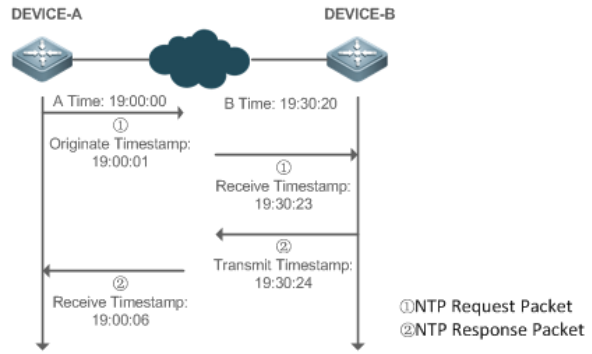
Working Principle

NTP time synchronization is implemented by interaction of NTP packets between a client and a server:

- The client sends a time synchronization packet to all servers every 64 seconds. After receiving response packets from the servers, the client filters and selects the response packets from all servers, and synchronizes time with an optimum server.
- After receiving the time synchronization request packet, a server uses the local clock as the reference source, and fills the local time information into the response packet to be sent to the client based on the protocol requirement.

Figure 3-4 shows the format of an NTP time synchronization packet.

Figure 3-4 Working Principle of NTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an NTP client that synchronizes time with DEVICE-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.
2. After a 2-second network delay, 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 2-second network delay, 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 obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

NTP Working Mode

- External clock reference mode

In this mode, a device is used as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server first and provide time synchronization for the clients after successful synchronization.

- Local clock reference mode

In this mode, a device uses the default local clock as the reliable clock source and provides time synchronization directly for other clients.

Related Configuration

Configuring an NTP Server

- The NTP function is disabled by default.
- Run the **ntp server** command to specify an NTP server (external clock reference source), which can enable NTP.
- After the configuration, the device works in the external clock reference mode.

Real-time Synchronization

- A device performs time synchronization every 64 seconds by default.

Updating a Hardware Clock

- By default, a device does not update synchronized time to the hardware clock.
- Run the **ntp update-calendar** command to enable a device to automatically update the hardware clock after successfully synchronizing time each time.

Configuring the NTP Master Clock

- By default, a device works in the external clock reference mode.
- Run the **ntp master** command to configure a device to the local clock reference mode.

2.3.2 NTP Security Authentication

To prevent malicious damage on an NTP server, NTP uses the authentication mechanism to check whether the time synchronization information is really from the announced server and check the information return path to provide an anti-interference protection mechanism.

Working Principle

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.

Related Configuration

↘ **Configuring a Global Security Authentication Mechanism for NTP**

- By default, no NTP security authentication mechanism is enabled.
- Run the **ntp authenticate** command to enable the NTP security authentication mechanism.

↘ **Configuring a Global Authentication Key for NTP**

- By default, no global authentication key is configured.
- Run the **ntp authentication-key** command to enable an NTP global authentication key.

↘ **Configuring a Globally Trusted Key ID for NTP**

- By default, no globally trusted key is configured.
- Run the **ntp trusted-key** command to configure a device as the reference clock source to provide a trusted key for time synchronization externally.

↘ **Configuring a Trusted Key ID for an External Reference Clock Source**

- Run the **ntp server** command to specify an external reference source and the trusted key of this clock source as well.

2.3.3 NTP Access Control

Working Principle

Provide a minimum security measure by using an ACL.

Related Configuration

↘ **Configuring the Access Control Rights for NTP Services**

- By default, there is no access control right for NTP.
- Run the **ntp access-group** command to configure the access control rights for NTP.

2.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of NTP	(Mandatory) It is used to enable NTP. After NTP is enabled, a device works in the external clock reference mode.	
	ntp server	Configures an NTP server.
	ntp update-calendar	Automatically updates a hardware clock.
	(Optional) It is used to configure a device to the local clock reference mode.	
	ntp master	Configures the NTP master clock.
	(Optional) It is used to disable NTP.	
	no ntp	Disables all functions of NTP and clears all NTP configurations.
	ntp disable	Disables receiving of NTP packets from a specified interface.
Configuring NTP Security Authentication	(Optional) It is used to prevent unreliable clock sources from performing time synchronization interference on a device.	
	ntp authenticate	Enables a security authentication mechanism.
	ntp authentication-key	Configures a global authentication key.
	ntp trusted-key	Configures a trusted key for time synchronization.
	ntp server	Configures a trusted key for an external reference clock source.
Configuring NTP Access Control	(Optional) It is used to filter the sources of received NTP packets.	
	ntp access-group	Configures the access control rights for NTP.

2.4.1 Configuring Basic Functions of NTP

Configuration Effect

External Clock Reference Mode

- Use a device as a client to synchronize time from an external reference clock source to the local clock.
- After the time synchronization is successful, use the device as a time synchronization server to provide time synchronization.

Local Clock Reference Mode

- Use the local clock of a device as the NTP reference clock source to provide time synchronization.

Notes

- In the client/server mode, a device can be used as a time synchronization server to provide time synchronization only after successfully synchronizing time with a reliable external clock source.
- Once the local clock reference mode is configured, the system will not synchronize time with a clock source with a higher stratum.
- Configuring a local clock as the master clock (especially when specifying a lower stratum) may overwrite an effective clock source. If this command 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 system time configuration section in the configuration guide.

Configuration Steps

Configuring an NTP Server

- (Mandatory) At least one external reference clock source must be specified (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.

Automatically Updating a Hardware Clock

- Optional.
- By default, the system updates only the system clock, but not the hardware clock after successful time synchronization.
- After this command is configured, the system automatically updates the hardware clock after successful time synchronization.

Configuring the NTP Master Clock

- To switch a device to the local clock reference mode, run this command.

Disabling NTP

- To disable NTP and clear NTP configurations, run the **no ntp** command.
- By default, all interfaces can receive NTP packets after NTP is enabled. To disable NTP for a specified interface, run the **ntp disable** command.

Verification

- Run the **show ntp status** command to display the NTP configuration.

- Run the **show clock** command to check whether time synchronization is completed.

Related Commands

Configuring an NTP Server

Command	**ntp server**{*ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain*}[**version** *version*][**source** *if-name*][**key** *keyid*][**prefer**]
Parameter Description	*ip-addr*: Indicates the IPv4/IPv6 address of the reference clock source. *domain*: Indicates the IPv4/IPv6 domain name of the reference clock source. *version*: Indicates the NTP version number, ranging from 1 to 3. *if-name*: Indicates the interface type, including AggregatePort, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and Vlan. *keyid*: Indicates the key used for communicating with the reference clock source, ranging from 1 to 4294967295. **prefer**: Indicates whether the reference clock source has a high priority.
Command Mode	Global configuration mode
Usage Guide	By default, no NTP server is configured. client system 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. If it is necessary to configure an authentication key, you must configure NTP security authentication before configuring an NTP server. The default version of NTP for communicating with a server is NTP version 3. 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.

Updating a Hardware Clock

Command	**ntp update-calendar**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Local Reference Clock Source

Command	**ntp master**[*stratum*]
Parameter Description	*stratum*: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.
Command Mode	Global configuration mode

Usage Guide	N/A

Disabling NTP

Command	**no ntp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command can be used to fast disable all functions of NTP and clear all NTP configurations.

Disabling Receiving of NTP Packets on an Interface

Command	**ntp disable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

External Clock Reference Mode of NTP

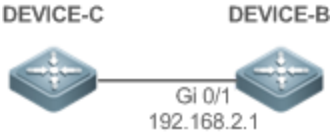
Scenario **Figure 3-5**	
	● DEVICE-B is configured to the NTP external clock reference mode. ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-A configures the local clock as the NTP reference clock source. ● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.

DEVICE-A	`A#configure terminal`
	`A(config)# ntp master`
	`A(config)#exit`

DEVICE-B	`B#configure terminal`
	`B(config)# ntp server 192.168.1.1`
	`B(config)# exit`

DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show ntp status** command on DEVICE-B to display the NTP configuration. ● DEVICE-B sends a time synchronization packet to 192.168.1.1 in order to synchronize time with DEVICE-A. ● After successfully synchronizing time with DEVICE-A, DEVICE-B can respond to the time synchronization request from DEVICE-C. ● Run the **show clock** command on DEVICE-B and DEVICE-C to check whether the time synchronization is successful.

Local Clock Reference Mode of NTP

Scenario **Figure 3-6**	
	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp master B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful.

2.4.2 Configuring NTP Security Authentication

Configuration Effect

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.

Notes

The authentication keys of the client and server must be the same.

Configuration Steps

Configuring a Global Security Authentication Mechanism for NTP

- Mandatory.
- By default, a device disables the security authentication mechanism.

Configuring a Global Authentication Key for NTP

- Mandatory.
- By default, a device is not configured with an authentication key.

Configuring a Globally Trusted Key ID for NTP

- Optional.
- 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.

Configuring an Authentication Key ID for an External Reference Clock Source

- Optional.
- 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.

Verification

- Run the **show run** command to verify the NTP configuration.
- Run the **show clock** command to check whether time is synchronized only with a trusted device.

Related Commands

Enabling a Security Authentication Mechanism

Command	**ntp authenticate**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	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.

Configuring a Global Authentication Key

Command	**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]
Parameter Description	*key-id*: indicates the ID of a global authentication key, ranging from 1 to 4294967295. *key-string*: indicates a key string. *enc-type*: (optional) indicates whether an entered key is encrypted. 0 indicates no encryption, and 7 indicates simple encryption. The default setting is no encryption.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for NTP

Command	**ntp trusted-key** *key-id*
Parameter Description	*key-id*: Indicates the ID of a trusted key, ranging from 1 to 4294967295.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for an External Reference Clock Source

Refer to the section “Related Commands”.

Configuration Example

Security Authentication

Scenario Figure 3-7	
	● DEVICE-B is configured to the NTP client/server mode and provides NTP services requiring security authentication for DEVICE-C. The authentication key is "abcd". ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.

DEVICE-B	B#configure terminal B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
Verification	● DEVICE-B sends a time synchronization packet that carries authentication information to 192.168.1.1 in order to synchronize time with DEVICE-A. ● Run the **show clock** command on DEVICE-B to check whether the time synchronization is successful.

2.4.3 Configuring NTP Access Control

Configuration Effect

Access control for NTP services provides a minimum security measure. A more secure method is to use an NTP authentication mechanism.

Notes

- Currently, the system does not support control query (used to control NTP servers by using network management devices, such as setting the leap second indicator or monitoring its working status). Though rule matching is implemented in the preceding sequence, no request related to control query is supported.
- If no access control rule is configured, all accesses are allowed. If any access control rule is configured, only accesses allowed by the rule can be implemented.

Related Configuration

↘ Configuring the Access Control Rights for NTP

- Optional.
- Run the **ntp access-group** command to configure the access control rights and a corresponding ACL for NTP.

Verification

Run the **show run** command to verify the NTP configuration.

Related Commands

Configuring the Access Control Rights for NTP Services

Command	**ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** } { *access-list-number* | *access-list-name* }
Parameter Description	**peer**: allows time request and control query for local NTP services, and allows a local device to synchronize time with a remote system (full access rights). **serve**: allows time request and control query for local NTP services, but does not allow a local device to synchronize time with a remote system. **serve-only**: allows only time request for local NTP services. **query-only**: allows only control query for local NTP services. *access-list-number*: indicates the number of an IP ACL, ranging from 1 to 99 and from 1300 to 1999. For details about how to create an IP ACL, refer to the *Configuring ACL*. *access-list-name*: indicates the name of an IP ACL. For details about how to create an IP ACL, refer to the *Configuring ACL*.
Command Mode	Global configuration mode
Usage Guide	Configure NTP access control rights. When an access request arrives, the NTP service matches rules in the sequence from the minimum access restriction to the maximum access restriction and uses the first matched rule. The matching sequence is peer, serve, serve-only, and query-only.

Configuration Example

Configuring NTP Access Control Rights

Configuration Steps	Allow only the device with the IP address of 192.168.1.1 to send a time synchronization request to a local device.
	`Hostname(config)# access-list 1 permit 192.168.1.1` `Hostname(config)# ntp access-group serve-only 1`

2.5 Monitoring

Displaying

Description	Command
show ntp status	Displays current NTP information.

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
debug ntp	Enables debugging.
no debug ntp	Disables debugging.

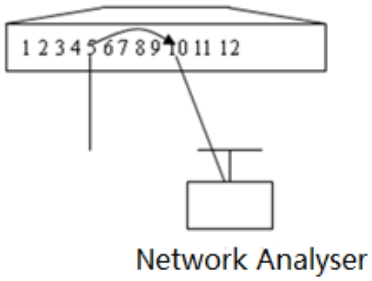
3 Configuring SPAN and RSPAN

3.1 Overview

The Switched Port Analyzer (SPAN) is to copy packets of a specified port to another switch port that is connected to a network monitoring device, so as to achieve network monitoring and troubleshooting.

All input and output packets of a source port can be monitored through SPAN. For example, as shown in the following figure, all packets on Port 5 are mapped to Port 10, and the network analyzer connected to Port 10 receives all packets that pass through Port 5.

Figure 5-1 SPAN Configuration Instance



The SPAN function is mainly applied in network monitoring and troubleshooting scenarios, to monitor network information and rectify network faults.

The Remote SPAN (RSPAN), an extension to SPAN, is capable of remotely monitoring multiple devices. Each RSPAN session is established in a specified remote VLAN. RSPAN breaks through the limitation that a mirrored port and a mirroring port must reside on the same device, and allows a mirrored port to be several network devices away from a mirroring port. Users can observe data packets of the remote mirrored port by using an analyzer in the central equipment room.

The application scenarios of RSPAN are similar to those of SPAN. RSPAN allows users to conduct real-time data monitoring without staying in the equipment room, providing great convenience for users.

3.2 Applications

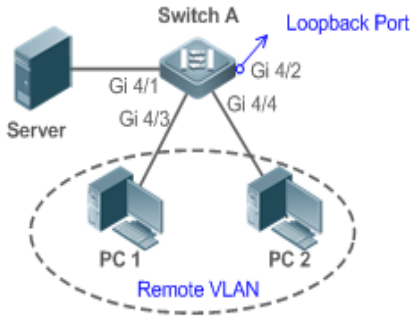
Application	Description
One-to-Many RSPAN	Multiple users need to monitor data of the same port.
RSPAN Basic Applications	Packets on the mirroring source device need to be mirrored to the destination device for monitoring.

3.2.1 One-to-Many RSPAN

Scenario

As shown in the following figure, one-to-many RSPAN can be implemented on a single device, that is, both PC 1 and PC 2 can be configured to monitor the transmitted and received traffic of the port connected to the server. Users can make proper configuration (for example, remote VLAN and port MAC loopback) to monitor data streams that pass through port Gi 4/1 on PC 1 and PC 2, thereby monitoring data streams of the server.

Figure 5-2 Application Topology of One-to-Many RSPAN



Deployment

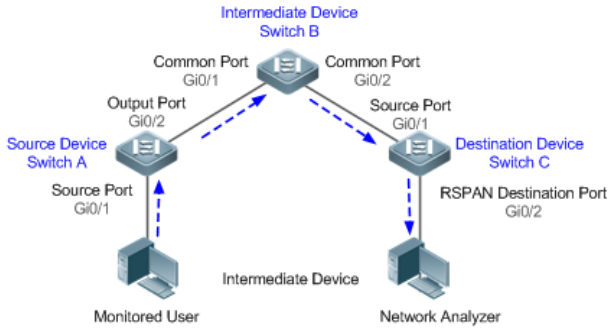
- Create a remote VLAN on Switch A.
- Configure Switch A as the source device of RSPAN and configure the port Gi 4/1 that is directly connected to the server as the RSPAN source port. Select a port that is in the Down state, Gi 4/2 in this example, as the RSPAN output port, add this port to the remote VLAN, and configure MAC loopback (run the **mac-loopback** command in interface configuration mode).
- Add ports that are directly connected to PC 1 and PC 2 to the remote VLAN.

3.2.2 RSPAN Basic Applications

Scenario

As shown in the following figure, the RSPAN function enables the network analyzer to monitor the STA connected to the source device Switch A from the destination device Switch C through the intermediate device Switch B. The devices can normally exchange data with each other.

Figure 5-3 Basic Application Topology of RSPAN



Deployment

- Configure a remote VLAN on Switch A, Switch B, and Switch C.
- On Switch A, configure port Gi 0/1 directly connected to the STA as the source port, configure port Gi 0/2 connected to Switch B as the output port, and configure the switching function for the output port.
- On Switch B, configure port Gi 0/1 connected to Switch A and port Gi 0/2 connected to Switch C as common ports.
- On Switch C, configure port Gi0/1 connected to Switch B as a common source port, configure port Gi 0/2 connected to the network analyzer as the RSPAN destination port, and configure the switching function for the RSPAN destination port.

3.3 Features

Basic Concepts

SPAN Session

A SPAN session is data streams between the SPAN source port and the destination port, which can be used to monitor the packets of one or more ports in the input, output, or both directions. Switched ports, routed ports, and aggregate ports (APs) can be configured as source ports or destination ports of SPAN sessions. Normal operations on a switch are not affected after ports of the switch are added to a SPAN session.

Users can configure a SPAN session on a disabled port but the SPAN session is inactive. A SPAN session is in the active state only after the port on which the SPAN session is configured is enabled. In addition, a SPAN session does not take effect after a switch is powered on. It is active only after the destination port is in the operational state. Users can run the **show monitor** [**session** *session-num*] command to display the operation status of a SPAN session.

SPAN Data Streams

A SPAN session covers data streams in three directions:

- Input data streams: All packets received by a source port are copied to the destination port. Users can monitor input packets of one or more source ports in a SPAN session. Some input packets of a source port may be discarded for some reasons (for example, for the sake of port security). It does not affect the SPAN function and such packets are still mirrored to the destination port.

- Output data streams: All packets transmitted by a source port are copied to the destination port. Users can monitor output packets of one or more source ports in a SPAN session. Packets transmitted from other ports to a source port may be discarded for some reasons and such packets will not be transmitted to the destination port. The format of output packets of a source port may be changed for some reasons. For example, after routing, packets transmitted from the source port are changed in source MAC addresses, destination MAC addresses, VLAN IDs, and TTLs, and their formats are also changed after copied to the destination port.
- 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.

Source Port

A source port is called a monitored port. In a SPAN session, data streams of the source port are monitored for network analysis and troubleshooting. In a single SPAN session, users can monitor the input, output, and bidirectional data streams, and the number of source ports is not restricted.

A source port has the following features:

- A source port can be a switched port, routed port, or AP.
- A source port cannot be used as a destination port simultaneously.
- A source port and a destination port can belong to the same VLAN or different VLANs.

Destination Port

A SPAN session has one destination port (called a monitoring port) for receiving packets copied from a source port.

A destination port has the following features:

- A destination port can be a switched port, routed port, or AP.
- A destination port cannot be used as a source port simultaneously.

CPU SPAN

CPU SPAN is to monitor packets transmitted from the CPU. Common SPAN monitors forwarded packets of a source port, excluding packets that are actively transmitted by the CPU to the source port. For example, for packets generated when a device actively pings another device, common SPAN cannot monitor the ping packets on the transmit device, unless the port of the receive device is configured as a source port for monitoring. CPU SPAN can directly monitor such packets generated when a device actively pings another device.

CPU SPAN has the following features:

- CPU SPAN can be configured separately, that is, only packets transmitted by the CPU are monitored.
- CPU SPAN can be configured together with common SPAN, that is, common mirrored packets and CPU packets are monitored.

Overview

Feature	Description

SPAN	Configures mirroring of ports on the same device.
RSPAN	Configures mirroring of ports on different devices.

3.3.1 SPAN

SPAN is used to monitor data streams on switches. It copies frames on one port to another switch port that is connected to a network analyzer or RMON analyzer so as to analyze the communication of the port.

Working Principle

When a port transmits or receive packets, SPAN, after checking that the port is configured as a SPAN source port, copies the packets transmitted and received by the port to the destination port.

↘ Configuring a SPAN Source Port

Users need to specify a SPAN session ID and source port ID to configure a SPAN source port, and set the optional SPAN direction item to determine the direction of SPAN data streams or specify an ACL policy to mirror specific data streams.

↘ Configuring a SPAN Destination Port

Users need to specify a SPAN session ID and destination port ID to configure a SPAN destination port, and set the optional switching function item to determine whether to enable the switching function and tag removal function on the SPAN destination port.

Related Configuration

The SPAN function is disabled by default. It is enabled only after a session is created, and the SPAN source and destination ports are configured. A SPAN session can be created when a SPAN source port or destination port is configured.

↘ Configuring a SPAN Source Port

A SPAN session does not have a SPAN source port by default. Users can run the following command to configure a SPAN source port:

monitor session *session-num* **source interface** *interface-id* [**both** | **rx** | **tx**]

In the preceding command:

session-num: Indicates the SPAN session ID. The number of supported SPAN sessions varies with products.

interface-id: Indicates the SPAN source port to be configured.

rx: Indicates that only packets received by the source port are monitored after **rx** is configured.

tx: Indicates that only packets transmitted by the source port are monitored after **tx** is configured.

both: Indicates that packets transmitted and received by the source port are copied to the destination port for monitoring after **both** is configured, that is, **both** includes **rx** and **tx**. If none of **rx**, **tx**, and **both** is selected, **both** is enabled by default.

↘ Configuring a SPAN Destination Port

A SPAN session does not have a SPAN destination port by default. Users can run the following command to configure a SPAN destination port:

monitor session *session-num* **destination interface** *interface-id* [**switch**]

In the preceding command:

switch: When you configure the SPAN destination port, if this option is enabled, the port receives both packets mirrored from the SPAN source port and packets from non-source ports. That is, the communication between this destination port and other devices is not affected.

3.3.2 RSPAN

RSPAN is capable of monitoring multiple devices. Each RSPAN session is established in a specified remote VLAN. RSPAN breaks through the limitation that a mirrored port and a mirroring port must reside on the same device, and allows a mirrored port to be several network devices away from a mirroring port.

Working Principle

A remote VLAN is created for the source device, intermediate device, and destination device, all ports involved in an RSPAN session need to be added to the remote VLAN. Mirrored packets are broadcasted in the remote VLAN so that they are transmitted from the source port of the source switch to the destination port of the destination switch.

↘ Configuring a Remote VLAN

Packets from an RSPAN source port are broadcasted in a remote VLAN so as to be copied from the local switch to the remote switch. The RSPAN source port, output port, reflection port, transparent transmission ports of the intermediate device (packet input port and output port of the intermediate device), destination port and input port of the destination port must be added to the remote VLAN. The RSPAN function requires configuring a VLAN as a remote VLAN in VLAN mode.

↘ Configuring an RSPAN Session

The configuration of the RSPAN source port and destination port are similar to that of the SPAN source port and destination port, but the mirroring session ID specified during configuration must be the ID of an RSPAN session.

↘ Configuring an RSPAN Source Port

The configuration of an RSPAN source port is the same as that of a SPAN source port, but the specified mirroring session ID must be the ID of an RSPAN session.

↘ Configuring an RSPAN Output Port

The output port is located on the source device and must be added to a remote VLAN. Mirrored packets of a source port are broadcasted in this remote VLAN. The source device transmits packets to the intermediate switch or destination switch through the output port.

↘ Configuring an RSPAN Destination Port

When an RSPAN destination port is configured, an RSPAN session ID, remote VLAN, and port name must be specified so that packets from the source port are copied to the destination port through the remote VLAN.

↘ Configuring Stream-based RSPAN

RSPAN is an extension to SPAN and also supports stream-based mirroring. The configuration is the same as that of stream-based SPAN. Stream-based RSPAN does not affect normal communication.

Users can configure an ACL in the input direction of a source port on an RSPAN source device. Standard ACLs, extended ACLs, MAC ACLs, and user-defined ACLs are supported.

Users can configure a port ACL in the input direction of a source port on an RSPAN source device, and configure a port ACL in the output direction of the destination port on the RSPAN destination device. Users can also configure an ACL in the output direction of a remote VLAN on an RSPAN source switch and configure an ACL in the input direction of the remote VLAN on the RSPAN destination switch.

Configuring One-to-Many RSPAN

If data streams of one source port need to be mirrored to multiple destination ports, users can configure an RSPAN session, configure the source port of the RSPAN session as a one-to-many mirroring source port and select another Ethernet port as the forwarding port (output port on the source device). In addition, the MAC loopback function needs to be configured on the RSPAN forwarding port in interface configuration mode, the expected RSPAN output port and RSPAN forwarding port need to be added to the remote VLAN. Then, mirrored packets are looped back on the RSPAN forwarding port and then broadcasted in the remote VLAN, thereby implementing one-to-many RSPAN.

Related Configuration

The RSPAN function is disabled by default. It is enabled only after an RSPAN session is created, and a remote VLAN, RSPAN source port, and RSPAN destination port are configured.

Configuring a Remote VLAN

No remote VLAN is specified for RSPAN by default. Users can run the **remote-span** command in VLAN mode to configure a VLAN as a remote VLAN. One remote VLAN corresponds to one RSPAN session.

Configuring an RSPAN Source Device

This function is disabled by default. Users can run the **monitor session** *session-num* **remote-source** command in global configuration mode to configure a device as the remote source device of a specified RSPAN session.

Configuring an RSPAN Destination Device

This function is disabled by default. Users can run the **monitor session** *session-num* **remote-destination** command in global configuration mode to configure a device as the remote destination device of a specified RSPAN session.

Configuring an RSPAN Source Port

A source port of an RSPAN session is configured on the source device. The configuration is the same as that of a SPAN source port but an RSPAN session ID needs to be specified. This function is disabled by d efault.

Configuring an Output Port on the RSPAN Source Device

This function is disabled by default. Users can run the **monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-name* **switch** command in global configuration mode to configure an output port on the RSPAN source device. The output port must be added to a remote VLAN.

Configuring a Destination Port on the RSPAN Destination Device

This function is disabled by default. Users can run the **monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-name* **switch** command in global configuration mode to configure a destination port on the RSPAN destination device. The destination port must be added to a remote VLAN.

Pay attention to the following points when using RSPAN:

A remote VLAN must be configured on each device, their VLAN IDs must be consistent, and all ports that participate in a session must be added to the VLAN.

It is not recommended that common ports be added to a remote VLAN.

Do not configure a port that is connected to an intermediate switch or destination switch as an RSPAN source port. Otherwise, traffic on the network may be in chaos.

3.4 Configuration

Configuration	Description and Command	
Configuring SPAN Basic Functions	(Mandatory) It is used to create SPAN.	
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Configures a SPAN source port.
	monitor session *session-num* **destination interface** *interface-id* **switch**	Configures a SPAN destination port.
Configuring RSPAN Basic Functions	(Mandatory) It is used to create RSPAN.	
	monitor session *session-num* **remote-source**	Configures an RSPAN session ID and specifies a source device.
	monitor session *session-num* **remote-destination**	Configures an RSPAN session ID and specifies a destination device.
	remote-span	Configures a remote VLAN.
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Configures an RSPAN source port.
	monitor session *session-num* **destination remote vlan** *remote-vlan-id* **interface** *interface-id* [**switch**]	Configures an output port on the RSPAN source device or a destination port on the RSPAN destination device.

3.4.1 Configuring SPAN Basic Functions

Configuration Effect

- Configure a source and destination ports for a SPAN session.
- Configure a destination port to monitor any packets transmitted and received by a source port.

Notes

- If a source port or destination port is added to an AP, the source port or destination port exits from a SPAN session.

Configuration Steps

Configuring a SPAN Session

- Global configuration mode. Mandatory.
- You can configure a SPAN session when configuring a SPAN source port or destination port.

Configuring a SPAN Source Port

- Global configuration mode. Mandatory.
- You can select the SPAN direction when configuring a SPAN source port. The **both** direction is configured by default, that is, both transmitted and received packets are monitored.

Configuring a SPAN Destination Port

Global configuration mode. Mandatory.

A SPAN session is active only when a SPAN source port is configured and a SPAN destination port is configured.

Verification

- Run the **show monitor** command or the **show running** command to verify the SPAN configuration. Alternatively, conduct packet capture analysis on the SPAN destination port and check whether the SPAN function takes effect according to the captured packets.

Related Commands

Configuring a SPAN Source Port

Command	**monitor session** *session-num* **source interface** *interface-id* [**both** | **rx** |**tx**]
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id:* Indicates the interface ID. **both:** Indicates that packets in the input and output directions are monitored. It is the default value. **rx:** Indicates that packets in the input direction are monitored. **tx:** Indicates that packets in the output direction are monitored.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuring a SPAN Destination Port

Command	**monitor session** *session-num* **destination interface** *interface-id*[**switch**]
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id*: Indicates the interface ID. **switch:** Indicates that the switching function is enabled on the SPAN destination port. It is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

The following uses SPAN as an example.

Scenario Figure 5-4	
Configuration Steps	● As shown in Figure 5-5, add ports Gi 0/1 and Gi 0/2 of Device A to VLAN 1. ● Create SVI 1 and set the address of SVI 1 to 10.10.10.10/24. ● Set IP addresses of PC 1 and PC 2 to 10.10.10.1/24 and 10.10.10.2/24 respectively. ● Configure SPAN for Device A and configure ports Gi 0/1 and Gi 0/2 as the source port and destination port of SPAN respectively.

A	`Hostname# configure`
	`Hostname(config)# vlan 1`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# interface vlan 1`
	`Hostname(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0`
	`Hostname(config-if-VLAN 1)# exit`
	`Hostname(config)# monitor session 1 source interface gigabitEthernet 0/1`
	`Hostname(config)# monitor session 1 destination interface gigabitEthernet 0/2`

Verification	Run the **show monitor** command to check whether SPAN is configured correctly. After successful

	configuration, PC 1 sends ping packets to SVI 1 and PC 2 conducts monitoring by using the packet capture tool.
A	Hostname# show monitor sess-num: 1 span-type: LOCAL_SPAN src-intf: GigabitEthernet 0/1 frame-type Both dest-intf: GigabitEthernet 0/2

Common Errors

- The session ID specified during configuration of the SPAN source port is inconsistent with that specified during configuration of the SPAN destination port.
- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.

3.4.2 Configuring RSPAN Basic Functions

Configuration Effect

- Configure a source port and destination port on the source device of an RSPAN session and configure the destination port on the destination device.
- Configure the destination port on the RSPAN destination device to monitor any packets that are transmitted or received by the source port.

Notes

- If a source port or destination port is added to an AP, the source port or destination port exits from a SPAN session.
- If the switch function is disabled on an RSPAN destination port, the destination port receives only mirrored packets and discards other packets that pass through the port. After the switch function is enabled, the destination port can receive non-mirrored packets.
- All ports involved in RSPAN must be added to a remote VLAN.
- A remote VLAN must be created on an intermediate device and transparent transmission ports must be added to the remote VLAN.

Configuration Steps

↘ Configuring an RSPAN Session

- Global configuration mode. Mandatory.
- The same session ID needs to be configured on the RSPAN source device and RSPAN destination device.

Configuring an RSPAN Source Device

- Global configuration mode. Mandatory.
- It is used to specify a device to be monitored by RSPAN.

Configuring an RSPAN Destination Device

- Global configuration mode. Mandatory.
- It is used to specify the destination device for outputting RSPAN packets.

Configuring an RSPAN Source Port

- Global configuration mode. Mandatory.
- Complete the configuration on an RSPAN source device. After configuration, RSPAN monitoring can be conducted on packets of the RSPAN source port. You can specify RSPAN to monitor remote VLAN packets in the input direction, output direction, or both directions of the RSPAN source port.

Configuring an RSPAN Output Port

- Global configuration mode. Mandatory.
- Complete the configuration on an RSPAN source device. After configuration, mirrored packets received by the ports added to the remote VLAN can be transmitted to the RSPAN destination device through the output port.
- The loopback port and output port are required for the one-to-many RSPAN, while the one-to-one RSPAN requires only output port.

Configuring an RSPAN Destination Port

- Global configuration mode. Mandatory.
- Complete the configuration on the RSPAN destination device. After configuration, the RSPAN destination device forwards mirrored packets received by the ports added to the remote VLAN to the monitoring device through the destination port.

Verification

- Run the **show monitor** command or the **show running** command to check whether RSPAN is successfully configured on each device, or conduct packet capture on the destination mirroring port on the RSPAN destination device to check whether packets mirrored from the source port of the RSPAN source device are captured.

Related Commands

Configuring an RSPAN Source Device

Command	**monitor session** *session-num* **remote-source**
Parameter Description	*session-num:* Indicates the ID of an RSPAN session.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Configuring an RSPAN Destination Device

Command	**monitor session** *session-num* **remote-destination**
Parameter Description	*session-num:* Indicates the ID of an RSPAN session.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Remote VLAN

Command	**remote-span**
Parameter Description	N/A
Command Mode	VLAN mode
Usage Guide	N/A

Configuring an RSPAN Source Port

Command	**monitor session** *session-num* **source interface** *interface-id* [**both | rx | tx**]
Parameter Description	*session-num:* Indicates the ID of an RSPAN session. *interface-id:* Indicates the interface ID. **both**: Indicates that packets in the input and output directions are monitored. It is the default value. **rx**: Indicates that packets in the input direction are monitored. **tx**: Indicates that packets in the output direction are monitored.
Command Mode	Global configuration mode
Usage Guide	The configuration is the same as that of a SPAN source port but an RSPAN session ID needs to be specified.

Configuring an Output Port on the RSPAN Source Device

Command	**monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-id* **switch**
Parameter Description	*session-num:* Indicates the ID of an RSPAN session. *remote-vlan*: Indicates a remote VLAN. *interface-id:* Indicates the interface ID. **switch**: Indicates whether the port participates in packet switching.
Command Mode	Global configuration mode
Usage Guide	The loopback port and output port are required for the one-to-many RSPAN, while the one-to-one RSPAN

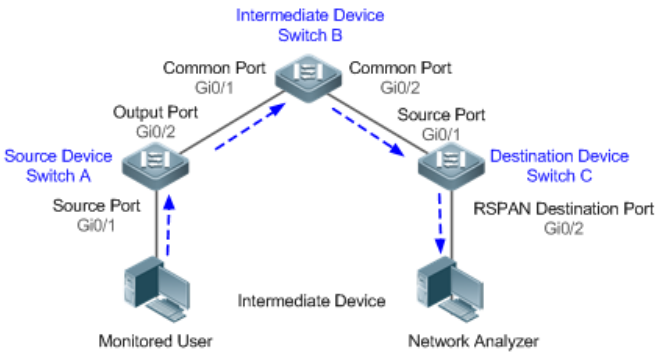
	requires only output port.

Configuring a Destination Port on the RSPAN Destination Device

Command	**monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-id* **switch**
Parameter Description	*session-num:* Indicates the ID of an RSPAN session. *remote-vlan*: Indicates a remote VLAN. *interface-id:* Indicates the interface ID. ***switch***: Indicates whether the port participates in packet switching.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring RSPAN

Scenario Figure 5-5	
Configuration Steps	● As shown in the preceding figure, configure a remote VLAN on the source device Switch A, intermediate device Switch B, and destination device Switch C. ● Configure the RSPAN source device, specify the source port, output port and loopback port on Switch A. ● Add ports Gi0/1 and Gi0/2 to the remote VLAN on Switch B. ● Configure the RSPAN destination device and specify the destination port on Switch C.

A	`Hostname# configure`
	`Hostname(config)# vlan 7`
	`Hostname(config-vlan)# remote-span`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# monitor session 1 remote-source`
	`Hostname(config)# monitor session 1 source interface fa 0/1 both`

	Hostname(config)# monitor session 1 destination remote vlan 7 interface fa 0/2 switch Hostname(config)# interface fa0/2 Hostname(config-if)# mac-loopback Hostname(config-if)# switchport access vlan 7 Hostname(config-if)# exit Hostname(config)# interface range fa0/3-4 Hostname(config-if-range)# switchport mode trunck
B, C	Hostname(config)# vlan 7 Hostname(config-vlan)# remote-span Hostname(config-vlan)# exit Hostname(config)# monitor session 1 remote-destination Hostname(config)# monitor session 1 destination remote vlan 7 interface fa 0/2 Hostname(config)# interface fa0/1 Hostname(config-if)# switchport mode trunck
Verification	Run the **show monitor** command or the **show running** command on Switch A, Switch B, and Switch C to check whether RSPAN is configured successfully.
A	Hostname# 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
B	! vlan 1 remote-span ! !

	interface GigabitEthernet 0/1 switchport mode trunk ! Interface GigabitEthernet 0/2 switchport mode trunk !
C	Hostname# show monitor sess-num: 1 span-type: DEST_SPAN dest-intf: GigabitEthernet 0/2 Remote vlan 7 mtp_switch on

Common Errors

- A remote VLAN must be configured on the source device, intermediate device, and destination device, and their VLAN IDs must be consistent.
- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.
- One MAC loopback port and multiple output ports need to be configured to implement one-to-many RSPAN.

3.5 Monitoring

Displaying

Description	Command
Displays all mirroring sessions existing in the system.	**show monitor**
Displays a specified mirroring session.	**show monitor session** *session-id*

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs SPAN.	**debug span**

4 Configuring sFlow

4.1 Overview

sFlow is a network monitoring technology jointly developed by InMon, HP, and FoundryNetworks in 2001. This technology has been standardized. It can provide complete traffic flows of Layer 2 to Layer 4, and it is applicable to traffic analysis in the extra-large network. This technology helps users analyze the performance, trend, and existence of network traffic flows in a detailed manner in real time.

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.

Protocol Specification

- sFlow Version 5
- RFC 1014

4.2 Applications

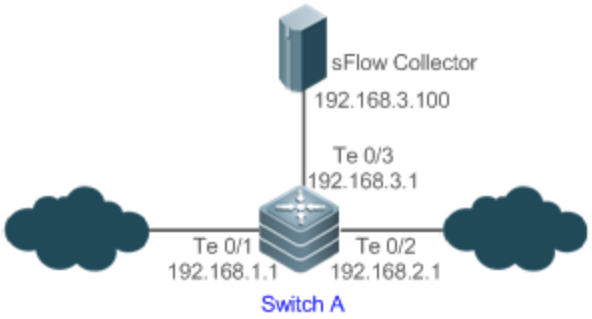
Typical Application	Scenario
Monitoring the LAN Traffic	Regard the device as an sFlow Agent, perform sampling of interface traffic in the LAN, and send the sFlow datagrams to an sFlow Collector for traffic analysis, thereby achieving the purpose of network monitoring.

4.2.1 Monitoring the LAN Traffic

Application Scenario

As shown in Figure 7-1, start switch A that serves as an sFlow Agent, enable flow sampling and counter sampling on port Te 0/1, monitor the traffic in the 192.168.1.0 network segment, encapsulate the sampling data into sFlow datagrams at regular intervals or when the buffer is full, and sent the sFlow data to the sFlow Collector for traffic analysis.

Figure 7-1



Function Deployment

- Configure the addresses of sFlow Agent and sFlow Collector on switch A.
- Enable flow sampling and counter sampling on port Te 0/1 of switch A.

Lots of server software supports sFlow. You can obtain software supporting sFlow at http://www.sflow.org/products/collectors.php. The software sflowtrend is free of charge.

4.3 Features

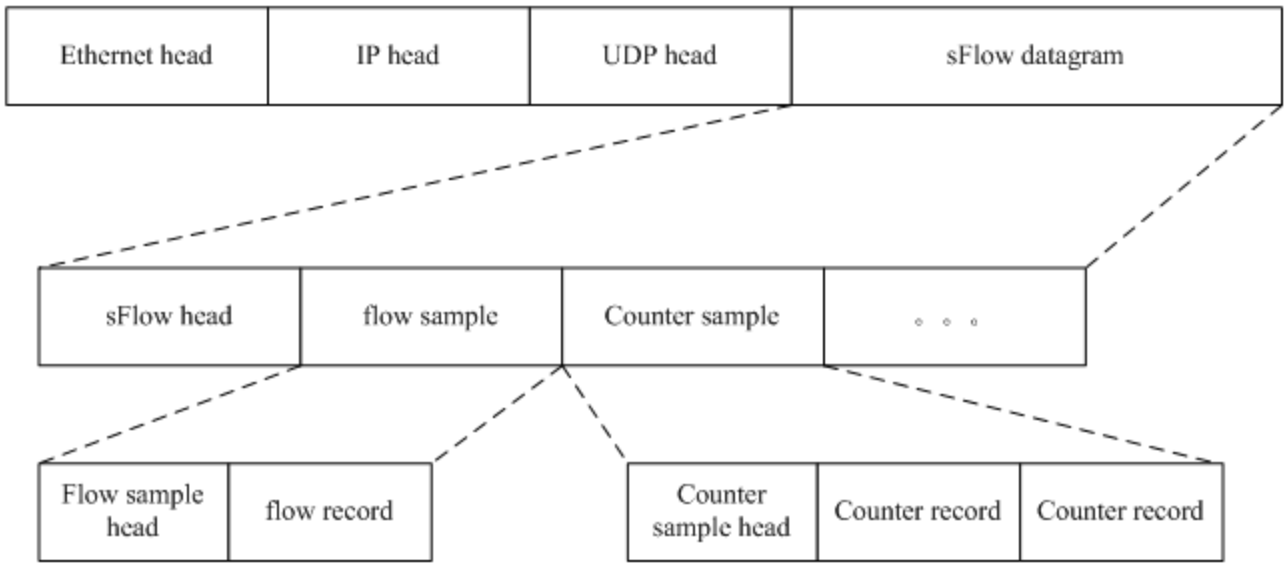
Basic Concepts

sFlow Agent

sFlow Agent is embedded in a network device. Generally, one network device can serves as an sFlow Agent. sFlow Agent can perform flow sampling and counter sampling, encapsulate sampled data into sFlow datagrams, and send the sFlow datagrams to the sFlow Collector.

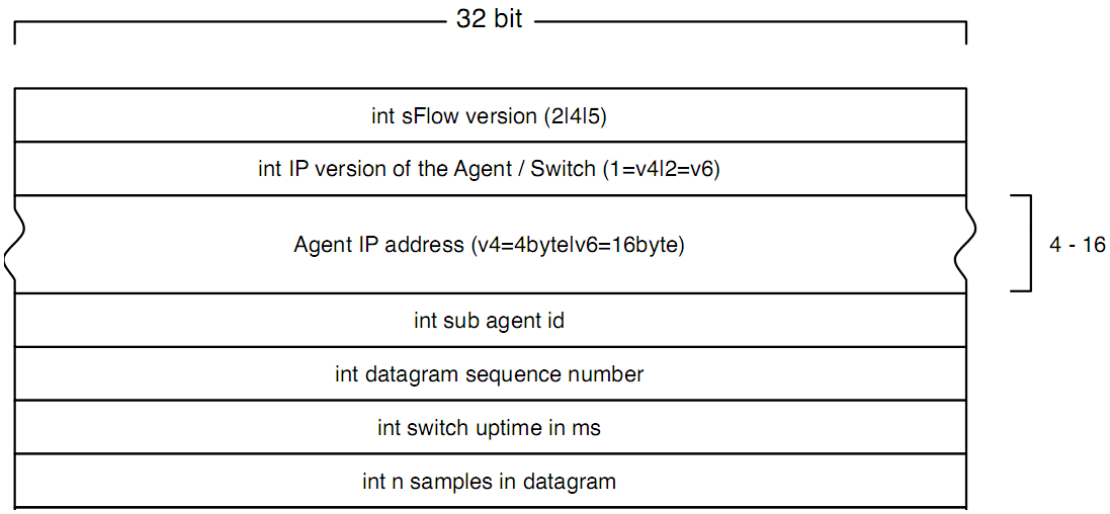
sFlow datagrams are encapsulated in UDP. Figure 7-2 shows the sFlow datagram format.

Figure 7-2 sFlow Datagram Format



One sFlow datagram may contain one or multiple flow samples and counter samples.

Figure 7-3 sFlow Header



sFlow Geader 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 the sFlow datagram
Switch uptime	Duration from the startup time of the switch to the current time
n samples in datagram	The number of samples in the an sFlow datagram. One sFlow datagram may contain one or multiple flow samples and counter samples.

sFlow Collector

sFlow Collector receives and analyzes the sFlow datagram sent from the sFlow Agent. sFlow Collector may be a PC or server. A PC or server installed with the application software for sFlow datagram analysis can be regarded as an sFlow Collector.

Flow Sampling

Based on the specified sampling rate, the sFlow Agent device performs flow sampling on the traffic flowing through an interface, including copying the header of the packet, extracting the Ethernet header and IP header of the packet, and obtaining the route information of the packet.

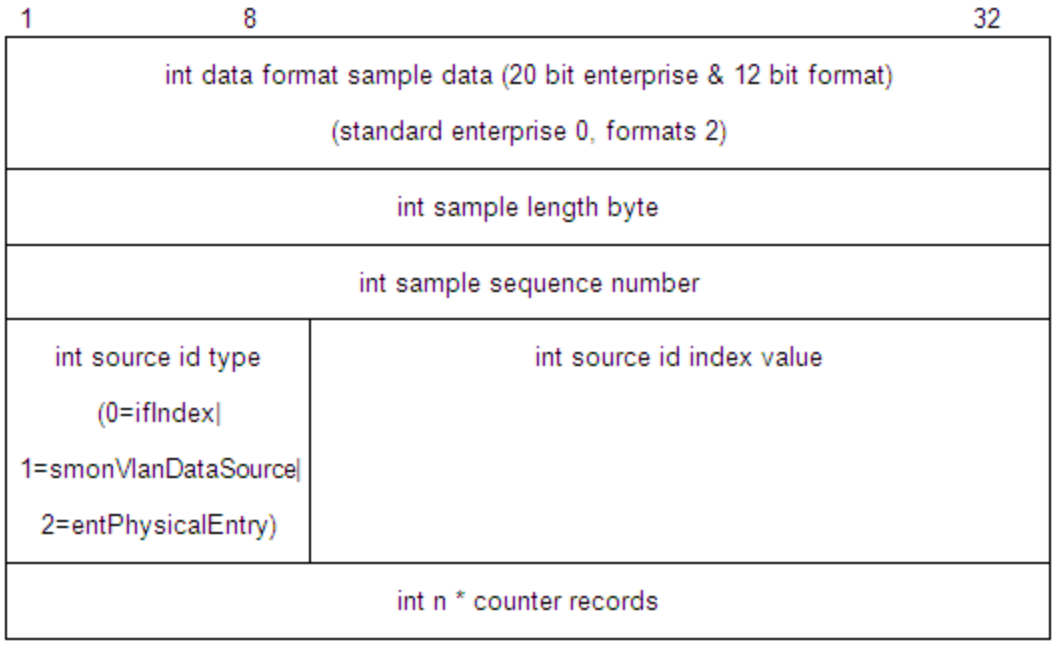
Figure 7-4 Flow Sample Header

1 8 32	
int data format sample data (20 bit enterprise & 12 bit format) (standard enterprise 0, formats 1)	
int sample length byte	
int sample sequence number	
int source id type (0=ifIndex| 1=smonVlanDataSource| 2=entPhysicalEntry)	int source id index value
int sampling rate	
int sample pool (total number of packets that could have been sampled)	
int drops (packets dropped due to a lack of resources)	
int input (SNMP ifIndex of input interface, 0 if not known)	
int output (SNMP ifIndex of output interface, 0 if not known) broadcast or multicast are handled as follows: the first bit indicates multiple destinations, the lower order bits number of interfaces	
int n * flow records	

Counter Sampling

In counter sampling, an sFlow Agent periodically obtains the statistics and CPU usage on a specified interface. The statistics on the interface include the number of packets input through the interface and the number of packets output through the interface.

Figure 7-5 Counter Sample Header



Functions and Features

Feature	Description
Flow Sampling	Sample the traffic flowing through the interface, and send the encapsulated sFlow datagram to the sFlow Collector for analysis.
Counter Sampling	Periodically send the statistics on the interface to the sFlow Collector for analysis.

4.3.1 Flow Sampling

Sample the traffic flowing through the interface, and send the encapsulated sFlow datagram to the sFlow Collector for analysis.

Working Principle

Based on the specified sampling rate, the sFlow Agent device performs flow sampling on the traffic flowing through an interface, including copying the header of the packet, extracting the Ethernet header and IP header of the packet, and obtaining the route information of the packet. Then, the sFlow Agent encapsulates the flow sampling data into an sFlow datagram and sends the datagram to the sFlow Collector for analysis.

4.3.2 Counter Sampling

Periodically send the statistics on the interface to the sFlow Collector for analysis.

Working Principle

The sFlow Agent performs interface polling on a regular basis. For an interface whose counter sampling interval expires, the sFlow Agent obtains the statistics on this interface, encapsulates the statistics into an sFlow datagram, and sends the datagram to the sFlow Collector for analysis.

4.4 Configuration

Configuration Item	Suggestion & Related Command	
Configuring Basic Functions of sFlow	⚠ Mandatory configuration. Establish communication connections between sFlow Agent and sFlow Collector.	
	sflow agent {address | interface}	Configures the sFlow Agent address.
	sflow collector *collector-id* **destination**	Configures the sFlow Collector address.
	⚠ Mandatory configuration. Enable flow sampling and counter sampling.	
	sflow counter collector	Enables the sFlow Agent to send counter samples to the sFlow Collector.
	sflow flow collector	Enables the sFlow Agent to send flow samples to the sFlow Collector .
	sflow enable	Enables sFlow sampling for the configuration interface, that is, enables counter sampling and flow sampling.
Configuring Optional Parameters of sFlow	⚠ Optional configuration. Sets the optional parameter attributes of sFlow.	
	sflow collector *collector-id* **max-datagram-size**	Configures the maximum length of the sFlow datagram.
	sflow counter interval	Configures the counter sampling interval.
	sflow flow max-header	Configures the maximum length of the packet header copied during flow sampling.
	sflow sampling-rate	Configures the sampling rate of flow sampling.

4.4.1 Configuring Basic Functions of sFlow

Configuration Effect

- 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.

Notes

- Flow sampling can be configured on only physical interfaces.
- To enable the sFlow Collector to analyze the flow sampling results, the IP address of the sFlow Collector on the sFlow Agent device is required.

Configuration Steps

Configuring sFlow Agent Address

- Mandatory configuration.
- Use the **sflow agent address** command to configure the address of the sFlow Agent.
- The sFlow Agent address must be a valid address. That is, the sFlow Agent address must not be a multicast or broadcast address. It is recommended that the IP address of the sFlow Agent device be used.

Command	**sflow agent** { **address** {*ipv4-address* **| ipv6** *ipv6-address* } } | { **interface** { *interface-name* | **ipv6** *interface-name* } }
Parameter Description	**address**: Configures the IP address of the sFlow agent. *Ipv4-address*: sFlow Agent IPv4 address **ipv6** *ipv6-address*: sFlow Agent IPv6 address **interface**: Configures the interface of the sFlow agent. *interface-name*: Interface of IPv4 address. **ipv6** *interface-name*: Interface of IPv6 address.
Defaults	No sFlow Agent address is configured by default
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the **Agent IP address** field in the output sFlow datagram. The datagram not configured with this filed cannot be output. The sFlow Agent address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Agent address, a message indicating configuration failure is displayed. It is recommended that the IP address of the sFlow Agent device be configured as the sFlow Agent address.

Configuring sFlow Collector Address

- Mandatory configuration.
- Use the **sflow collector** command to configure the address of the sFlow Collector.
- The sFlow Collector address must be a valid address. That is, the sFlow Collector address must not be a multicast or broadcast address. sFlow Collector must exist, and the route to it must be reachable.

Command	**sflow collector** *collector-id* **destination** { *ipv4-address* | **ipv6** *ipv6-address* } *udp-port*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2. *Ipv4-address*: sFlow Agent IPv4 address. It is not configured by default

	ipv6 *ipv6-address*: sFlow Agent IPv6 address. It is not configured by default *udp-port*: sFlow Collector listening port number
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the sFlow Collector address. The sFlow Collector address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Collector address, a message indicating configuration failure is displayed. The sFlow Collector monitors the sFlow datagram on the specified port.

Enabling sFlow Samples Output to the sFlow Collector

- Mandatory configuration.
- You can use the **sflow flow collector** command to enable the sFlow Agent to send flow samples to the sFlow Collector.
- This function must be enabled on the interface to send flow samples to the sFlow Collector. In addition, sFlow Collector must exist, the route to it must be reachable, and the IP address of the corresponding sFlow Collector has been configured on the sFlow Agent device.

Command	**sflow flow collector** *collector-id*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2.
Defaults	Sending the flow samples to the sFlow Collector is disabled by default.
Command Mode	Interface configuration mode
Configuration Usage	This command can be used for physical ports and aggregated ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Enabling Counter Samples Output to the sFlow Collector

- Mandatory configuration.
- You can use the **sflow counter collector** command to enable the sFlow Agent to send counter samples to the sFlow Collector.
- This must be enabled on the interface to send counter samples to the sFlow Collector. In addition, sFlow Collector must exist, the route to it must be reachable, and the IP address of the corresponding sFlow Collector has been configured on the sFlow Agent device.

Command	**sflow counter collector** *collector-id*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2.
Defaults	Sending counter samples to the sFlow Collector is disabled by default.

Command Mode	Interface configuration mode
Configuration Usage	This command can be used for physical ports and aggregated ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.

Enabling Counter Sampling and Flow Sampling

- Mandatory configuration.
- You can use the **sflow enable** command to enable the flow sampling and counter sampling on an interface.
- The forwarding performance of an interface may be affected after flow sampling is enabled.

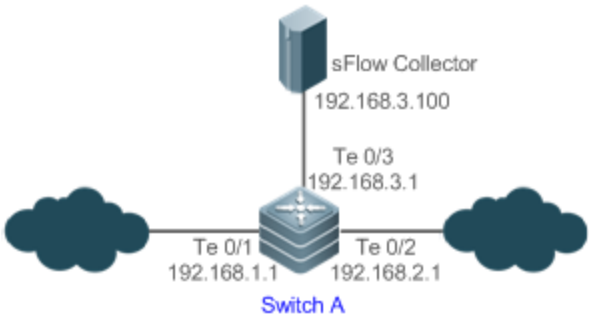
Command	**sflow enable**
Parameter Description	
Defaults	The sFlow sampling function on an interface is disabled by default.
Command Mode	Interface configuration mode
Configuration Usage	This command can be used to enable counter sampling and flow sampling for physical ports

Verification

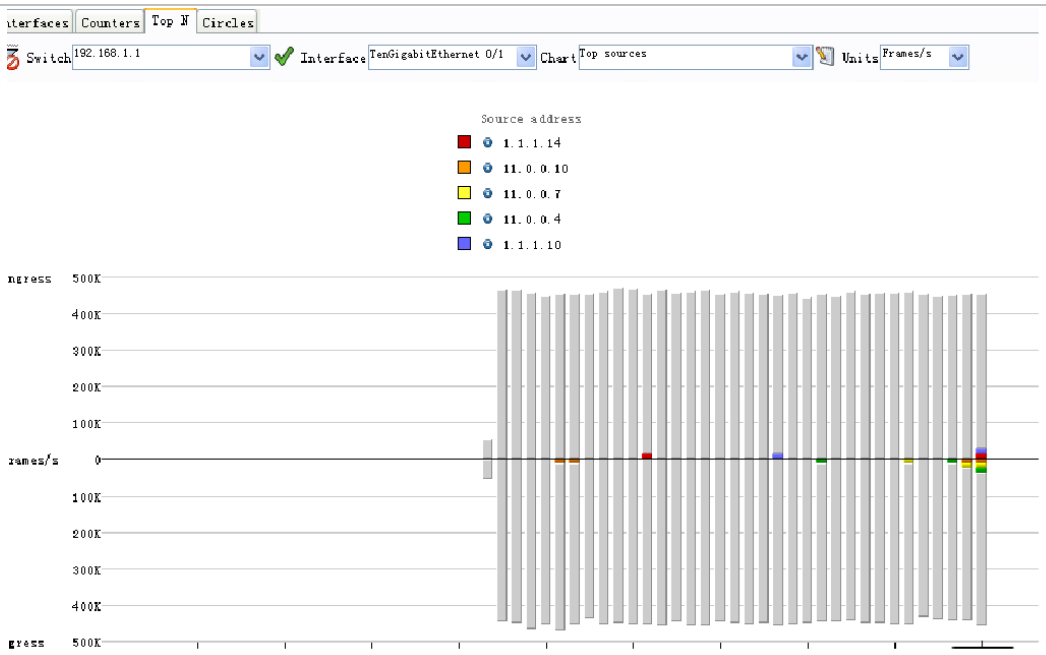
- Use the **show sflow** command to display the sFlow configuration, and check whether the displayed information is consistent with the configuration.

Configuration Examples

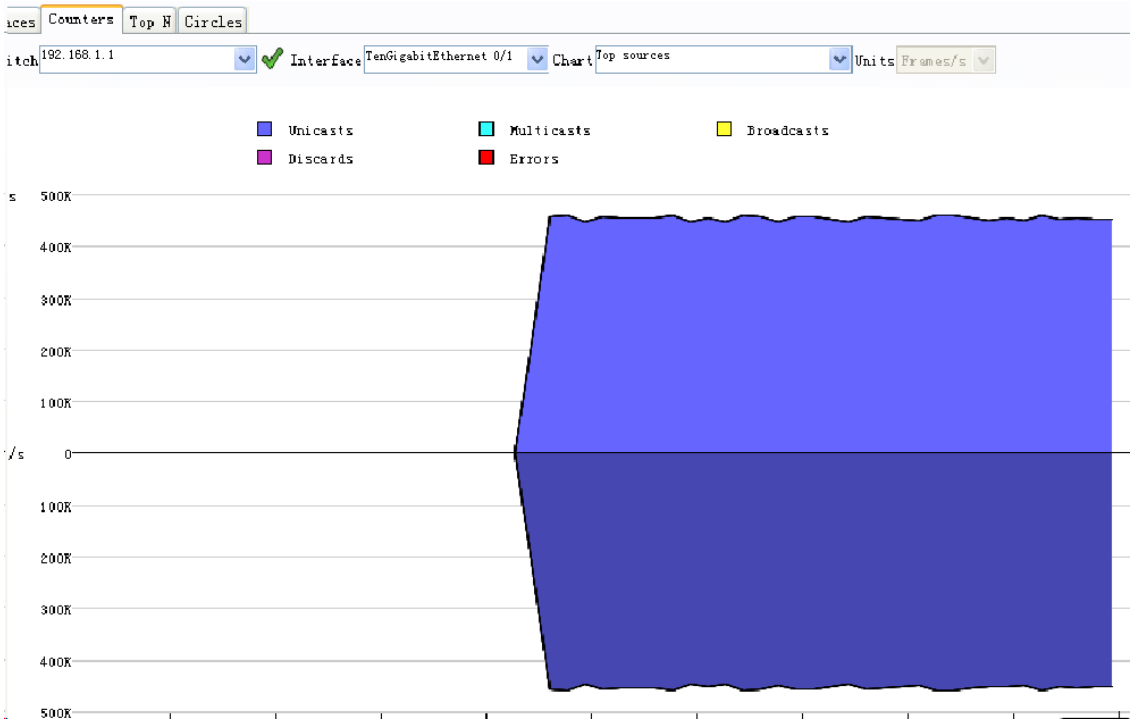
Configuring Flow Sampling and Counter Sampling for sFlow Agent

Scenario Figure 7-6	
	As shown in Figure 7-6, start switch A that serves as the sFlow Agent, enable flow sampling and counter sampling on port Te 0/1, monitor the traffic in the 192.168.1.0 network segment, encapsulate the sampling traffic into sFlow datagrams at regular intervals or when the buffer is full, and send the sFlow datagrams to the sFlow Collector for traffic analysis.

Configuration Steps	● Configure 192.168.1.1 as the sFlow Agent address. ● Configure 192.168.3.100 as the address of sFlow Collector 1, and 6343 as the port number. ● Configure interface TenGigabitEthernet 0/1 to output flow samples and counter samples to sFlow Collector 1, and enable the sFlow sampling function on this interface.
Switch A	Hostname# configure terminal Hostname(config)# sflow agent address 192.168.1.1 Hostname(config)# sflow collector 1 destination 192.168.3.100 6343 Hostname(config)# interface TenGigabitEthernet 0/1 Hostname(config-if-TenGigabitEthernet 0/1)# sflow flow collector 1 Hostname(config-if-TenGigabitEthernet 0/1)# sflow counter collector 1 Hostname(config-if-TenGigabitEthernet 0/1)# sflow enable Hostname(config-if-TenGigabitEthernet 0/1)# end
Verification	Use the **show sflow** command to check whether the command output is consistent with the configuration.
	Hostname# show sflow sFlow datagram version 5 Global information: Agent IP: 192.168.1.1 sflow counter interval:30 sflow flow max-header:64 sflow sampling-rate:8192 Collector information: ID IP Port Size VPN 1 192.168.3.100 6343 1400 2 NULL 0 1400 Port information Interface CID FID Enable TenGigabitEthernet 0/1 1 1 Y Information displayed on the sFlowTrend software:



The preceding figure shows the Top N page of the sFlowTrend software. This page displays the flow sampling results and displays the top 5 source IP addresses that involve the largest traffic. The total incoming traffic is about 450 Kpps and the total outgoing traffic is 450 Kpps, which are consistent with the actual traffic.



The preceding figure shows the counters page of the sFlowTrend software. This page displays the counter

	sampling results. The incoming traffic is 450 Kpps and the outgoing traffic is also 450 Kpps. In addition, all packets are unicast packets.

4.4.2 Configuring Optional Parameters of sFlow

Configuration Effect

You can adjust the data sampling accuracy by modifying relevant parameter attributes of sFlow.

Notes

- The forwarding performance may be affected when the sampling rate is too low.

Configuration Steps

↘ Configuring the Maximum Length of the Output sFlow Datagram

- Optional configuration.
- You can use the **sflow collector** command to configure the length of the sFlow datagram, excluding the Ethernet header, IP header, and UDP header. An sFlow datagram may contain one or multiple flow samples and counter samples. Configuration of the output sFlow datagram's maximum length may lead to the result that the number of sFlow datagrams output during processing of a certain number of flow samples differs from the number of sFlow datagrams output during processing of the same number of counter packets. If the maximum length is greater than MTU, the output sFlow datagrams will be segmented.

Command	**sflow collector** *collector-id* **max-datagram-size** *datagram-size*
Parameter Description	*collector-id*: sFlow Collector ID. The range is from 1 to 2 **max-datagram-size** *datagram-size*: maximum length of the output sFlow datagram. The range is from 200 to 9,000.
Defaults	The default value is 1,400.
Command Mode	Global configuration mode
Configuration Usage	-

↘ Configuring the Flow Sampling Rate

- Optional configuration.
- You can use the **sflow sampling-rate** command to configure the global flow sampling rate.
- Configuration of flow sampling rate my affect the sFlow sampling accuracy. A lower sampling rate means a higher accuracy and larger CPU consumption. Therefore, the forwarding performance of the interface may be affected when the sampling rate is low.

Command	**sflow sampling-rate** *rate*
Parameter Description	*rate*: Sampling rate of sFlow sampling. One packet is sampled from every *n* packets (*n* equals the value of **rate**). The range is from 4,096 to 65,535.

Defaults	The default global flow sampling rate is 8,192.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the global sampling rate of sFlow flow sampling, and sFlow flow sampling of all interfaces uses this sampling rate.

Configuring the Maximum Length of the Packet Header Copied During Flow Sampling

- Optional configuration.
- You can use the **sflow flow max-header** command to configure the length of the packet header copied during flow sampling globally.
- Users can use this command to modify the datagram information to be sent to the sFlow Collector. For example, if a user concerns about the IP header, this user can configure the length to 56 bytes. During encapsulation of flow samples, the first 56 bytes of the sample packet are copied to the sFlow datagram.

Command	**sflow flow max-header** l*ength*
Parameter Description	*length*: maximum length of the packet header to be copied. The range is from 18 to 256.
Defaults	The default length of the packet header to be copied during global flow sampling is 64 bytes.
Command Mode	Global configuration mode
Configuration Usage	Configure the maximum number of bytes of the packet content copied from the header of the original packet. The copied content is recorded in the generated sample.

Configuring the Sampling Interval

- Optional configuration.
- You can use the **sflow counter interval** command to configure the global counter sampling interval.
- Enable the counter sampling interface to send the statistics on it to the sFlow Collector at the sampling interval.

Command	**sflow counter interval** *seconds*
Parameter Description	*seconds*: time interval. The range is form 3 to 2,147,483,647. The unit is second.
Defaults	The default global counter sampling interval is 30 seconds.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval.

Verification

- Check whether an sFlow datagram with the flow samples is received on the sFlow Collector.
- Use the **show sflow** command to display the sFlow configuration, and check whether the displayed information is consistent with the configuration.

Configuration Examples

Configuring Optional Parameters of sFlow

Scenario	See Figure 7-6.
	• Set the flow sampling rate to 4,096 in global configuration mode. • Configure the length of the packet header copied during flow sampling to 128 bytes in global configuration mode. • Set the sampling interval to 10 in global configuration mode.
Configuration Steps	Hostname# configure terminal Hostname(config)# sflow sampling-rate 4096 Hostname(config)# sflow flow max-header 128 Hostname(config)# sflow counter interval 10
	Make traffic pass through interface TenGigabitEthernet 0/1. • Check whether there is traffic on interface TenGigabitEthernet 0/1 on sFlow Collector 1. • Use the **show sflow** command to check whether the command output is consistent with the configuration.
Verification	Hostname# show sflow sFlow datagram version 5 Global information: Agent IP: 10.10.10.10 sflow counter interval:10 sflow flow max-header:128 sflow sampling-rate:4096 Collector information: ID IP Port Size VPN 1 192.168.2.100 6343 1400 2 NULL 0 1400 Port information Interface CID FID Enable TenGigabitEthernet 0/1 0 1 Y

4.5 Monitoring

Displaying

Function	Command
Displays the sFlow configuration.	**show sflow**