



XS-S1930J Series Switches

RGOS Configuration Guide, Release 11.4(1)B70P15

Copyright Statement

Ruijie Networks©2021

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

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Thank you for using our products. This manual matches the RGOS Release 11.4(1)B70P15.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://case.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: [service_rj@ruijienetworks.com](https://www.skype.com/people/service_rj@ruijienetworks.com)

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.

{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols



Means reader take note. Notes contain helpful suggestions or references.



Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

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 CWMP
8. Configuring PoE

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

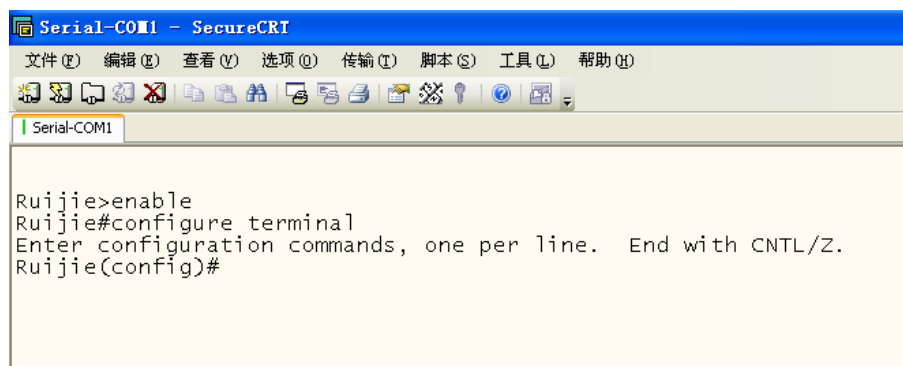


Remarks	A is the network device to be managed. PC is a terminal.
----------------	---

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 "Ruijie".

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.	Ruijie>	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.	Ruijie#	Run the disable command to return to User EXEC mode. Run the configure command to enter global configuration mode.	Use this command mode to check whether the 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.	Ruijie(config)#	Run the exit or end command, or press Ctrl+C to return to Privileged EXEC mode. Run the interface command to enter interface configuration mode. When using the interface command, you must specify the interface. Run the vlan <i>vlan_id</i> 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.	Ruijie(config-if)#	Run the end command, or press Ctrl+C to return to Privileged EXEC mode. Run the exit command to return to global configuration mode. 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 <i>vlan_id</i> command to enter VLAN configuration mode.	Ruijie(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

```
Ruijie>?
Exec commands:
<1-99>      Session number to resume
```

```

disable    Turn off privileged commands
disconnect Disconnect an existing network connection
enable     Turn on privileged commands
exit       Exit from the EXEC
help       Description of the interactive help system
lock       Lock the terminal
ping       Send echo messages
show       Show running system information
telnet     Open a telnet connection
traceroute Trace route to destination

```


2. 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

```

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

```

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

```

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

```

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

For example

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

4. 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

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

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

For example

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

1.3.4 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:

```
Ruijie(config)#int g0/1  
Ruijie(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.

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 editing line.	Left key or Ctrl+B	Move the cursor to the previous character.
	Right key or Ctrl+B	Move the cursor to the next character.

Function	Key or Short-Cut Key	Description
	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
$.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 <i>any-command</i> begin <i>regular-expression</i>	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 <i>any-command</i> exclude <i>regular-expression</i>	Filters the output of the show command. Except those containing the specified contents, all lines will be output.
show <i>any-command</i> include <i>regular-expression</i>	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.

```
Ruijie#show running-config | include interface
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 simply the 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".

2. 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.

 These default aliases cannot be deleted.

Configuring a Command Alias

Command	alias <i>mode command-alias original-command</i>
Parameter Description	<i>mode</i> : indicates the command mode of the command represented by the alias. <i>command-alias</i> : indicates the command alias. <i>original-command</i> : 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.

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 .
	<pre>Ruijie#configure terminal Ruijie(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1</pre>
Verification	<ul style="list-style-type: none"> ● Run the show alias command to check whether the alias is configured successfully. <pre>Ruijie(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</pre>
	<ul style="list-style-type: none"> ● Use the configured alias to run the command, and run the show running-config command to check whether the alias is configured successfully.
	<pre>Ruijie(config)#ir Ruijie(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</pre>

	!
--	---

📌 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.
	<pre>Ruijie#configure terminal Ruijie(config)#alias config ir ip route</pre>
Verification	<ul style="list-style-type: none"> ● Run the show alias command to check whether the alias is configured successfully. <pre>Ruijie(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route</pre>
	<ul style="list-style-type: none"> ● 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.
	<pre>Ruijie(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1 Ruijie(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 !</pre>

System Help

- The system provides help information for command aliases. 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.

```
Ruijie#s?
```

```
*s=show show start-chat start-terminal-service
```

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

For example, in Privileged EXEC mode, configure the alias "sv" to replace the **show version** command. If you enter "sv?", the keywords starting by "s" and alias information are displayed.

```
Ruijie#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.

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

```
A. B. C. D IP address
```

```
dhcp IP Address via DHCP
```

```
Ruijie(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).
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. It is recommended that a password be configured for security purposes.

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.
- Run the **login privilege log** command to enable the function of logging privilege change.

↘ Enabling Line Password Protection

- Line password protection is required for remote login (such as login through Telnet).
- Run the **password** { [0] *password* | 7 *encrypted-password* } 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 to configure non-AAA authentication on LINE.
- Perform this configuration on each 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 **Ruijie**. 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 **Ruijie**.

▾ **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 a Welcome Message**

- By default, no welcome message is configured.
- Run the **banner exec** command to configure a welcome message.

▾ **Configuring a Prompt Message for Reverse Telnet Session**

- By default, no prompt message for reverse Telnet session is configured.
- Run the **banner incoming** command to configure a prompt message for reverse Telnet session.

▾ **Configuring a Prompt-timeout Message**

- By default, no prompt-timeout message is configured.
- Run the **banner prompt-timeout** command to configure a prompt-timeout message to notify timeout.

▾ **Configuring a Message for SLIP/PPP session**

- By default, no message for SLIP/PPP session is configured.
- Run the **banner slip-ppp** command to configure a slip-ppp message for the SLIP/PPP session.

▾ **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.

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 Telnet

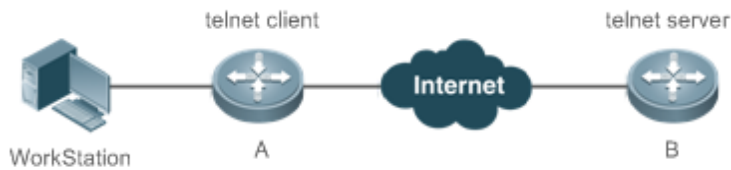
Working Principle

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 Figure2-2, 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.

Ruijie 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.

▾ Enabling the Do Telnet Client Service

- Run the **do 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.



▾ Configuring the source address for Telnet connection

- Run the **ip telnet source-interface** command to configure the IP address of an interface as the source address for global Telnet connection.

2.3.6 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.

2.3.7 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.
	login privilege log	Enables the function of logging privilege change.
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 Do Telnet 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.
	banner login	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 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.
- Run the **login privilege log** command to enable the function of logging privilege change.

↘ **Enabling Line Password Protection**

- (Optional) Line password protection is required for remote login (such as login through Telnet).
- Run the **password** { [0] *password* | 7 *encrypted-password* } 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 [<i>level level</i>] { <i>password</i> [0 7] <i>encrypted-password</i> }
Parameter	<i>level</i> : Indicates a specific user level.
Description	<p><i>password</i>: Indicates the password used to enter privileged EXEC mode.</p> <p>0: Indicates that the password is entered in plaintext.</p> <p>7: Indicates that the password is entered in cyphertext.</p> <p><i>encrypted-password</i>: Indicates the password text, which must contain case-sensitive English letters and digits.</p> <p> Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.</p>
Command Mode	Global configuration mode
Usage Guide	<p>Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured.</p> <p>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.</p> <p>If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed.</p> <p> 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.</p>


↘ **Configuring a Secure Encrypted Password**

Command	enable secret [level <i>level</i>] { [0] <i>password</i> 5 <i>encrypted-secret</i> }
Parameter Description	<i>level</i> : Indicates a specific user level. 0 5 : Indicates the password encryption type. 0 indicates no encryption, and 5 indicates secure encryption. <i>encrypted-secret</i> : 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 [<i>privilege-level</i>]
Parameter Description	<i>privilege-level</i> : 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 [<i>privilege-level</i>]
Parameter Description	<i>privilege-level</i> : 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 <i>privilege-level</i> is specified, the current privilege level is reduced to the specified level.  <i>privilege-level</i> must be lower than the current level.

↘ Enabling the Logging of Privilege Change

Command	login privilege log
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the logging of privilege change.

↘ Configuring Command Privilege Levels

Command	privilege mode [all] { level <i>level</i> reset } <i>command-string</i>
Parameter Description	<i>mode</i> : 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.

	<p>all: Changes the subcommand privilege levels of a specific command to the same level.</p> <p>level level: Indicates a privilege level, ranging from 0 to 15.</p> <p>reset: Restores the command privilege level to the default.</p> <p><i>command-string</i>: Indicates the command to be assigned a privilege level.</p>
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] password 7 encrypted-password }
Parameter Description	<p>0: Indicates the password is in plain text.</p> <p><i>password</i>: Indicates the password for remote line login.</p> <p>7: Indicates the password is encrypted.</p> <p><i>encrypted-password</i>: Indicates the password string.</p>
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	<ul style="list-style-type: none"> Assign privilege level 1 to the reload command and its subcommands. <pre>Ruijie# configure terminal Ruijie(config)# privilege exec all level 1 reload Ruijie(config)# enable secret level 1 0 test Ruijie(config)# end</pre>

Verification	<ul style="list-style-type: none"> Check whether the reload command and its subcommands are accessible at level 1.
	<pre>Ruijie# disable 1 Ruijie> reload ? at reload at<cr></pre>

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

- (Optional) When AAA is enabled, run the **login access non-aaa** command to configure non-AAA authentication on LINE.

- Perform this configuration on every device.
- ↳ **Enabling the Telnet Client Service**
- Run the **telnet** command to log in to a remote device.
- ↳ **Enabling the Do Telnet Client Service**
- Run the **do 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.
- ↳ **Importing/Exporting Local User Information**
- Optional.
- Run the **username import** or **username export** command to import user information from a text file or export user information to a text file.

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 <i>name</i> [login mode { aux console ssh telnet }] [online amount <i>number</i>] [permission <i>oper-mode path</i>] [privilege <i>privilege-level</i>] [reject remote-login] [web-auth] [nopassword password [0 7] <i>text-string</i>]
Parameter Description	<p><i>name</i>: Indicates a user name.</p> <p>login mode: Indicates the login mode.</p> <p>console: Sets the login mode to Console.</p> <p>ssh: Sets the login mode to SSH.</p> <p>telnet: Sets the login mode to Telnet.</p> <p>online amount <i>number</i>: Indicates the maximum number of online accounts.</p> <p>permission <i>oper-mode path</i>: Configures the file operation permission. <i>op-mode</i> indicates the operation mode, and <i>path</i> indicates the directory or path of a specific file.</p> <p>privilege <i>privilege-level</i>: Indicates the account privilege level, ranging from 0 to 15.</p> <p>reject remote-login: Rejects remote login by using the account.</p> <p>web-auth: Allows only Web authentication for the account.</p> <p>nopassword: Indicates that no password is configured for the account.</p> <p>password [0 7] <i>text-string</i>: 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.</p>
Command Mode	Global configuration mode
Usage Guide	<p>Use this command to create a local user database to be used by authentication.</p> <p>If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters.</p> <p>This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.</p>

↘ Configuring Local Authentication for Line-Based Login

Command	login local
Parameter	N/A
Description	
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	default: Indicates the default authentication method list name.
Description	<i>list-name:</i> 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 AAA Authentication for Line-Based Login

Command	login access non-aaa
Parameter	
Description	
Command Mode	Global configuration mode
Usage Guide	Use this command to configure non-AAA authentication on LINE when AAA is enabled.

↘ Enabling the Telnet Client Service

Command	telnet host [port] [/source { ip A.B.C.D interface interface-name }]
Parameter	<i>host:</i> Indicates the IPv4 address, IPv6 address, or host name of the Telnet server.
Description	<i>port:</i> Indicates the TCP port number of the Telnet server. The default value is 23. <i>/source:</i> 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. interface interface-name: Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, and IPv4 address.

↘ Enabling the DoTelnet Client Service

Command	do telnet host [port] [/source { ip A.B.C.D interface interface-name }]
----------------	--

Parameter Description	<p><i>host</i>: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server.</p> <p><i>port</i>: Indicates the TCP port number of the Telnet server. The default value is 23.</p> <p><i>/source</i>: Indicates the source IP address or source port used by a Telnet client.</p> <p>ip <i>A.B.C.D</i>: Indicates the source IPv4 address used by the Telnet client.</p> <p>interface <i>interface-name</i>: Indicates the source port used by the Telnet client.</p>
Command Mode	Privileged EXEC mode/configuration mode/interface configuration mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, and IPv4 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 <i>session-id</i>
Parameter Description	<i>session-id</i> : Indicates the suspended Telnet client session ID.
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.

↘ Configuring the Connection Timeout Time

Command	exec-timeout <i>minutes</i> [<i>seconds</i>]
Parameter Description	<p><i>minutes</i>: Indicates the connection timeout time in the unit of minutes.</p> <p><i>seconds</i>: Indicates the connection timeout time in the unit of seconds.</p>
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 <i>minutes</i> [output]
Parameter	<i>minutes</i> : Indicates the session timeout time in the unit of minutes.
Description	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	N/A
Description	
Command Mode	Line configuration mode
Usage Guide	N/A

▾ Locking a Terminal Connected to the Current Line

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

Configuration Example

▾ Establishing a Telnet Session to a Remote Network Device

Configuration Steps	<ul style="list-style-type: none"> Establish a Telnet session to a remote network device with the IP address 192.168.65.119. Run the telnet command in privileged EXEC mode, and run the do telnet command in privileged EXEC mode/configuration mode/interface configuration mode.
	<pre>Ruijie# telnet 192.168.65.119 Trying 192.168.65.119 ... Open User Access Verification Password:</pre>

	<pre>Ruijie(config)# do telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:</pre>
	<pre>Ruijie# telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:</pre>
Verification	<ul style="list-style-type: none"> ● Check whether the Telnet sessions are established to the remote network devices.

▾ Configuring the Connection Timeout Time

Configuration Steps	<ul style="list-style-type: none"> ● Set the connection timeout time to 20 minutes.
	<pre>Ruijie# configure terminal//Enter global configuration mode. Ruijie# line vty 0 //Enter line configuration mode. Ruijie(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.</pre>
Verification	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Set the session timeout time to 20 minutes.
	<pre>Ruijie# configure terminal//Enter global configuration mode. Ruijie(config)# line vty 0 //Enter line configuration mode. Ruijie(config-line)#session-timeout 20//Set the session timeout time to 20 minutes.</pre>
Verification	<ul style="list-style-type: none"> ● Check whether the session between a terminal and the local device is disconnected when no input is detected during the timeout time.

▾ Exporting Local User Information

Configuration Steps	<ul style="list-style-type: none"> ● Export user information to .csv file.
	<pre>Ruijie# username export user.csv</pre>

- | | |
|---------------------|---|
| Verification | <ul style="list-style-type: none">● Check whether the csv file can be generated successfully. |
|---------------------|---|

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 { <i>hour</i> [: <i>minute</i> [: <i>second</i>]] } [<i>month</i> [<i>day</i> [<i>year</i>]]]
Parameter Description	<i>hour</i> [: <i>minute</i> [: <i>second</i>]]: Indicates the current time, in the format of <i>hour</i> (24-hour format): <i>minute</i> : <i>second</i> . <i>month</i> : Indicates a month (from January to December) of the year. <i>day</i> : Indicates a day (1–31) of the month. <i>year</i> : Indicates a year, ranging from 1970 to 2037. 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 <i>name</i>
Parameter Description	<i>name</i> : 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 <i>string</i>
Parameter Description	<i>string</i> : 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 <i>c message c</i>
Parameter Description	<i>c</i> : 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 <i>c message c</i>
Parameter Description	<i>c</i> : 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 <i>speed</i>
Parameter Description	<i>speed</i> : 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	<ul style="list-style-type: none"> Change the system time to 2003-6-20, 10:10:12. <pre>Ruijie# clock set 10:10:12 6 20 2003 //Configure the system time and date.</pre>
Verification	<ul style="list-style-type: none"> Run the show clock command in privileged EXEC mode to display the system time. <pre>Ruijie# show clock //Confirm that the changed system time takes effect. clock: 2003-6-20 10:10:54</pre>

▾ Configuring Daily Notification

Configuration Steps	<ul style="list-style-type: none"> Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	<pre>Ruijie(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#'. Notice: system will shutdown on July 6th.# //Ending delimiter Ruijie(config)#</pre>
Verification	<ul style="list-style-type: none"> 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.
	<pre>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:</pre>

▾ Configuring a Login Banner

Configuration Steps	<ul style="list-style-type: none"> Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.
	<pre>Ruijie(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#'. Access for authorized users only. Please enter your password. # //Ending delimiter Ruijie(config)#</pre>
Verification	<ul style="list-style-type: none"> 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.
	<pre>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:</pre>

▾ Configuring the Serial Port Baud Rate

Configuration Steps	<ul style="list-style-type: none"> Set the serial port baud rate to 57,600 bps.
	<pre>Ruijie# configure terminal //Enter global configuration mode. Ruijie(config)# line console 0 //Enter console line configuration mode. Ruijie(config-line)# speed 57600 //Set the console baud rate to 57,600 bps. Ruijie(config-line)# end //Returns to privileged mode.</pre>
Verification	<ul style="list-style-type: none"> Run the show command to display the configuration.
	<pre>Ruijie# 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 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</pre>

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 service** command to display the service Enabled/Disable state.

Related Commands

▾ Enabling the Telnet Server, SNMP Agent, SSH Server, and Web Server Services

Command	enable service {telnet-server snmp-agent ssh-server web-server [http https all] }
Parameter Description	telnet-server: Enables or disables the Telnet Server service. snmp-agent: Enables or disables the SNMP Agent service. ssh-server: Enables or disables the SSH Server service. web-server: Enables or disables the Web Server 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	<ul style="list-style-type: none"> ● Enable the SSH Server service.
	<pre>Ruijie# configure terminal //Enter global configuration mode. Ruijie(config)#enable service ssh-server //Enable the SSH Server service.</pre>
Verification	<ul style="list-style-type: none"> ● 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 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	<code>reload [at { hh [:mm [:ss]] } [month [day [year]]]]</code>
Parameter	<code>at hh:mm:ss</code> : Indicates the time when the system will restart.
Description	<code>month</code> : Indicates a month of the year, ranging from 1 to 12. <code>day</code> : Indicates a date, ranging from 1 to 31. <code>year</code> : 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.

2.4.6 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	<code>execute { [flash:] filename }</code>
Parameter	<code>filename</code> : Indicates the path for the batch file to be executed.

Description	
Command	Privileged EXEC mode
Mode	
Usage Guide	Use this command to run the commands related to a function in batches.

2.5 Monitoring

Displaying

Description	Command
Displays the current system time.	show clock
Displays line configurations.	show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }
Displays debugging state.	show debugging
Displays system restart settings.	show reload
Displays the current running configurations of the device or the configurations on an interface.	show running-config
Display the service status.	show service
Display the Telnet Client session information.	show sessions
Displays the device configurations stored in the NVRAM.	show startup-config
Displays system information.	show version [devices module]
Displays the information of each established Telnet client instance.	show sessions

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	<p>console: Indicates the Console port.</p> <p>vtty: Indicates a virtual terminal line, which supports Telnet or SSH.</p> <p><i>first-line:</i> Indicates the number of the first line.</p> <p><i>last-line:</i> Indicates the number of the last line.</p>
Command Mode	Global configuration mode
Usage Guide	N/A

↘ **Increasing/Reducing the Number of VTY Lines**


Command	line vty <i>line-number</i>
Parameter Description	<i>line-number:</i> 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 <i>line-number</i> command to reduce the number of available VTY lines.

↘ **Displaying Line Configuration**

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

Configuration Example

↘ **Increasing the Number of VTY Terminals**

Scenario Figure 3-3	 <p>The diagram shows a laptop icon labeled 'PC' connected by a line to a server icon labeled 'A'.</p>
Configuration Steps	<ul style="list-style-type: none"> ● 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	<pre>Ruijie#show user</pre>

	<pre> Line User Host(s) Idle Location ----- * 0 con 0 --- idle 00:00:00 --- Ruijie#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 Ruijie#show line vty ? <0-5> Line number Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#line vty 35 Ruijie(config-line)# *Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console </pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● 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.
<p>A</p>	<pre>Ruijie#show line vty ?</pre>

```
<0-35> Line number

Ruijie#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 0/1
!
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
!
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 Hot Key for Terminal Service Disconnection**

- Optional.
- Run the **disconnect-character** command to configure the hot key to disconnect the terminal connection.

↘ **Configuring the Escape Character for the Line**

- Optional.
- Run the **escape-character** command to configure the escape character for the line.

↘ **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 Privilege Level for the Line

- Optional.
- Run the **privilege level** command to configure the privilege level for the line.

▾ Configuring the Login Refusal Message for the Line

- Optional.
- Run the **refuse-message** to configure the login refusal message for the line.

▾ 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 <i>minutes</i>
Parameter Description	<i>minutes</i> : 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 <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : 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 <i>autocommand-string</i>
Parameter Description	<i>autocommand-string</i> : 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 router 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 <i>bit</i>
Parameter Description	<i>bit</i> : 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 router 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 Hot Key for Terminal Service Disconnection

Command	disconnect-character <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : Indicates the ASCII decimal value of the hot key for terminal service disconnection. The value ranges from 0 to 255.
Command	Line configuration mode

Mode	
Usage Guide	This command is used to set the hot key that disconnects the terminal service connection. The hot key cannot be the commonly used ASCII node such as characters ranging from a to z, from A to Z or numbers ranging from 0 to 9. Otherwise, the terminal service will fail.

↘ Configuring the Escape Character for the Line

Command	escape-character <i>escape-value</i>
Parameter Description	<i>escape-value</i> : Indicates the ASCII value of the escape character. The value ranges from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	Configure this command, press the key combination of the escape character and then press x , the current session will be terminated and the line will return to the original session.

↘ 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. Ruijie general operating system (RGOS) 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 Privilege Level for the Line

Command	privilege level <i>level</i>
Parameter Description	<i>level:</i> Indicates the privilege level. The value ranges from 0 to 15.
Command Mode	Line configuration mode
Usage Guide	N/A

▾ Configuring the Login Refusal Message for the Line

Command	refuse-message [<i>c message c</i>]
Parameter Description	<i>c:</i> Indicates the delimiter of the login refusal message, which is not allowed within the message. <i>message:</i> Indicates the login refusal message.
Command Mode	Line configuration mode
Usage Guide	This command is used to configure the login refusal message for the line. The characters entered after the ending delimiter are discarded directly, The login refusal message is displayed when the user has been refused to login.

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

Command	start-character <i>ascii-value</i>
Parameter Description	<i>ascii-value:</i> 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 <i>ascii-value</i>
Parameter Description	<i>ascii-value:</i> Indicates the ASCII value of the stop character of software flow control for physical terminal connections. The value ranges from 0 to 255.
Command	Line configuration mode

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	1: Indicates one stop bit.
Description	2: Indicates two stop bits.
Command Mode	Line configuration 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 <i>terminal-type-string</i>
Parameter Description	<i>terminal-type-string</i> : 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	 <p>The diagram shows a laptop icon labeled 'PC' connected by a line to a server icon labeled 'A'.</p>
Configuration Steps	<ul style="list-style-type: none"> ● 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	<pre>Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#line console 0 Ruijie(config-line)#speed 115200</pre>

	<pre> Ruijie(config-line)#databits 8 Ruijie(config-line)#parity even Ruijie(config-line)#stopbits 1 Ruijie#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 </pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config command to display the configuration.
A	<pre> Ruijie#show line vty ? <0-35> Line number Ruijie#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 0/1 </pre>

```
!  
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  
  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 Escape Character for the Terminal

- Optional
- Run the **terminal escape-character** command to configure the escape character for 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 Escape Character for the Terminal**

- Optional.
- Run the **terminal escape-character** command to configure the escape character for the terminal.

↘ **Enabling Command History for the Terminal or Configuring the Number of Commands in the Command History**

- Optional.
- Run the **terminal history** command to enable command history for the terminal or configure the number of commands in the command history.

↘ **Configuring the Screen Length for the Terminal**

- Optional.
- Run the **terminal length** command to configure the screen length for the terminal.

↘ **Configuring the Location Description for the Terminal**

- Optional.
- Run the **terminal location** command to configure the location description for the terminal.

↘ **Configuring the Baud Rate for the Terminal**

- Optional.
- Run the **terminal speed** command to configure the baud rate for the terminal.

↘ **Configuring the Screen Width for the Terminal**

- Optional.
- Run the **terminal width** command to configure the screen width for the terminal.

↘ **Configuring the Authentication Timeout for the Terminal**

- Optional.
- Run the **timeout login** command to configure the authentication timeout for the terminal.

↘ **Configuring the Communication Protocol for the Terminal**

- Optional.
- Run the **transport input** command to configure the communication protocol for the terminal.

▾ Configuring the Logout Message for the Terminal

- Optional.
- ▾ Run the **vacant-message** command to configure the logout message for 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 EXEC Character Width for the Current Session

Command	terminal exec-character-bits { 7 8 }
Parameter	7: Selects the 7-bit ASCII character set.
Description	8: Selects the full 8-bit ASCII character set.
Command Mode	Privileged EXEC 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 Escape Character for the Terminal

Command	terminal escape-character <i>escape-value</i>
Parameter Description	<i>escape-value:</i> Configures the ASCII value corresponding to the escape character for the current terminal, The value ranges from 0 to 255.
Command Mode	Privileged EXEC mode
Usage Guide	After configuring this command, press the key combination of the escape character and then press x , the current session is disconnected to return to the original session.

↘ Enabling Command History for the Terminal or Configuring the Number of Commands in the Command History

Command	terminal history [size size]
Parameter Description	size size: Configures the number of commands. The value ranges from 0 to 256.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Screen Length for the Terminal

Command	terminal length <i>screen-length</i>
Parameter Description	<i>screen-length:</i> Configures the screen length. The value ranges from 0 to 512.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Location Description for the Terminal

Command	terminal location <i>location</i>
Parameter Description	<i>location:</i> Configures location description of the current device.

Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Baud Rate for the Terminal

Command	terminal speed <i>baudrate</i>
Parameter Description	<i>baudrate</i> : Configures the baud rate. The value ranges from 9600 to 115200.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Screen Width for the Terminal

Command	terminal width <i>screen-width</i>
Parameter Description	<i>screen-width</i> : Configures the screen width for the terminal, The value ranges from 0 to 256.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Configuring the Authentication Timeout for the Terminal

Command	timeout login response <i>seconds</i>
Parameter Description	response : Configures the time period during which the line waits for the user to enter any message. <i>seconds</i> : Timeout value in seconds. The value ranges from 1 to 300.
Command Mode	Line configuration mode
Usage Guide	N/A

↘ Configuring the Communication Protocol for the Terminal

Command	transport input { all telnet none }
Parameter Description	all : Allows all the protocols under Line to be used for communication. telnet : Allows only the Telnet protocol under Line to be used for communication. none : Allows none of protocols under line to be used for communication.
Command Mode	Line configuration mode
Usage Guide	N/A

↘ Configuring the Logout Message for the Terminal

Command	vacant-message [<i>c message c</i>]
Parameter	<i>c</i> : Indicates the delimiter of the logout message, which is not allowed within the message.

Description	<i>message</i> : Configures the logout message.
Command Mode	Line configuration mode
Usage Guide	This command is used to set the logout message for the line. The characters entered after the ending delimiter are discarded directly. The logout message is displayed when the user logs out.

▾ 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 <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : 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 <i>ascii-value</i>
Parameter Description	<i>ascii-value</i> : 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 <i>terminal-type-string</i>
Parameter Description	<i>terminal-type-string</i> : 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	 <p>The diagram shows a laptop icon labeled 'PC' connected by a line to a server icon labeled 'A'.</p>
Configuration Steps	<ul style="list-style-type: none"> 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	<pre>Ruijie#terminal terminal-type ansi Ruijie#terminal speed 115200</pre>
Verification	<ul style="list-style-type: none"> Run the show line console 0 command to display the status of the Console line.
A	<pre>Ruijie#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</pre>

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 <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }

Displaying

Description	Command
Displays the line configuration.	show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }
Display the command history of the line.	show history
Display the privilege level of the line.	show privilege
Display the login user information.	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 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.

4.2.1 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.

4.2.2 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.

4.3 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 <i>time-range-name</i> Configures a time range.
	 Optional configuration. You can configure various parameters as necessary.
	absolute { [start <i>time date</i>] [end <i>time date</i>] } Configures an absolute time range.
	periodic <i>day-of-the-week</i> <i>time</i> to [<i>day-of-the-week</i>] <i>time</i> Configures periodic time.

4.3.1 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	time-range <i>time-range-name</i>
Parameter	<i>time-range-name</i> : name of the time range to be created.
Description	
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	absolute { [start <i>time date</i>] [end <i>time date</i>] }
Parameter	start <i>time date</i> : start time of the range.
Description	end <i>time date</i> : 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	periodic <i>day-of-the-week time to [day-of-the-week] time</i>
Parameter	<i>day-of-the-week</i> : the week day when the periodic time starts or ends
Description	<i>time</i> : 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. It is recommended to disassociate time range before you change the periodic time and associate it again after you change the periodic time.

4.4 Monitoring and Maintaining Time Range

Displaying the Running Status

Description	Command
Displays time range configuration.	show time-range [<i>time-range-name</i>]

5 Configuring the 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 man-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

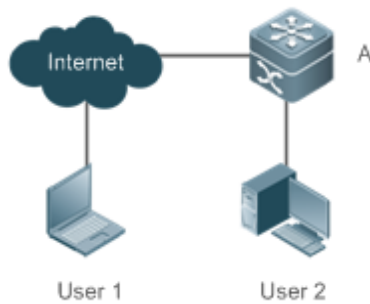
Scenario

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.
- 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	<p>A is a Ruijie device.</p> <p>User 1 accesses the device through the Internet.</p> <p>User 2 accesses the device through a LAN.</p>
----------------	---

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

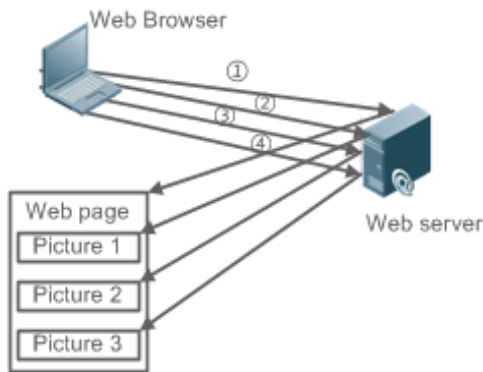
Basic Concepts

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.

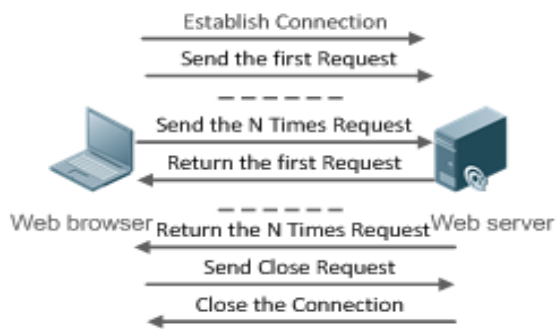
For example, a web page may need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is 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, Ruijie devices support both HTTP/1.0 and HTTP/1.1.

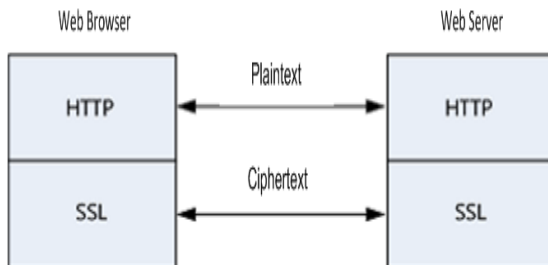
i Which HTTP version will be used by a device is decided by the Web browser.

⏏ 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



HTTP Upgrade Service

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.
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 Ruijie 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. 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 service 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 <i>privilege-level</i> username <i>name</i> password { <i>password</i> [0 7] <i>encrypted-password</i> }
Parameter Description	<p><i>privilege-level</i>: Permission level bound to a user.</p> <p><i>name</i>: User name.</p> <p><i>password</i>: User password.</p> <p>0 7: Password encryption type. 0: no encryption; 7: simple encryption. The default value is 0.</p> <p><i>encrypted-password</i>: Password text.</p>
Command Mode	Global configuration mode.
Usage Guide	<p>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.</p> <p>Run the no webmaster level <i>privilege-level</i> command to delete all user names and passwords of the specified permission level.</p> <p>Run the no webmaster level <i>privilege-level</i> username <i>name</i> command to delete the specified user name and password.</p> <hr/> <p> User names and passwords involve three permission levels: Up to 10 user names and passwords can be configured for each permission level.</p> <p> 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.</p>

↘ Configuring an HTTP Service Port

Command	http port <i>port-number</i>
Parameter Description	<i>port-number</i> : 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 <i>port-number</i>
Parameter Description	<i>port-number</i> : Configures an HTTPS service port. The value range is 443 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTPS service port.

Configuration Example

Managing one Ruijie Device by Using Web and Logging in to the Device 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 for access.
- The user is 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	<ul style="list-style-type: none"> ● 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	<pre>A#configure terminal A(config)# enable service web-server A(config)# http port 8080 A(config)# http secure-port 4430</pre>
Verification	Check HTTP configurations.
A	<pre>A# show web-server status http server status: enabled http server port: 8080 https server status:enabled https server port: 4430</pre>

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 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 web download tftp: <i>path</i>
Parameter	tftp: Connects the FFTP server through a common data port and downloads a Web package.
Description	<i>path:</i> 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 <i>uri</i>
Parameter	<i>uri:</i> Local path for storing a Web package.
Description	
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 5-6	 <p>The diagram shows a network device labeled 'A' on the left, connected by a line to a laptop labeled 'Web browser' on the right.</p>
Configuration Steps	<ul style="list-style-type: none"> ● 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.

	<ul style="list-style-type: none"> ● Log in to the device through Web and upload the latest Web package to the device.
A	<pre>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</pre>
	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 5-7	
Configuration Steps	<ul style="list-style-type: none"> ● 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	<pre>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.</pre>
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 5-8	
Configuration Steps	<ul style="list-style-type: none"> ● 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	<pre> 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. </pre>
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

6 Configuring Syslog

6.1 Overview

Status changes (such as link up and down) or abnormal events may occur anytime. Ruijie 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 syslog through the Console.
Sending Syslogs to the Log Server	Monitor syslog through the server.

6.2.1 Sending Syslogs to the Console

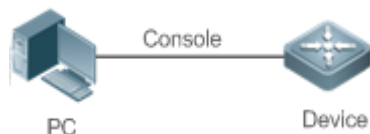
Scenario

Send syslog 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: Ruijie %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: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

The following describes each field in the log in details:

6. 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)

7. 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.

8. Timestamp

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

- i** 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.

9. 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.

10. 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.

11. Level

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

12. 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.

13. 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 ruijie SYS 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).

2. Version

According to RFC5424, the version is always 1.

3. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Ruijie 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".

4. 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.

5. 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.

6. Level

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

7. 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.

8. 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). Ruijie 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.

9. 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, 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* } [**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** } 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 does not generate 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 does not generate 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 [<i>message-type</i> [<i>uptime</i> <i>datetime</i> [<i>msec</i>] [<i>year</i>]]	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 [<i>level</i>]	Configures the level of logs displayed on the Console.
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 [<i>level</i>]	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 [<i>buffer-size</i>] [<i>level</i>]	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 { <i>ip-address</i> } [udp-port <i>port</i>]	Sends logs to a specified log server.
	logging trap [<i>level</i>]	Configures the level of logs sent to the log server.
	logging facility <i>facility-type</i>	Configures the facility value of logs sent to the log server.
	logging source [interface] <i>interface-type</i> <i>interface-number</i>	Configures the source interface of logs sent to the log server.

Configuration	Description and Command
	<p>logging source { ip <i>ip-address</i> }</p> <p>Configures the source address of logs sent to the log server.</p>
Writing Syslogs into Log Files	<p> (Optional) It is used to configure parameters for writing syslogs into a file.</p>
	<p>logging file flash:filename [<i>max-file-size</i>] [<i>level</i>]</p> <p>Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.</p>
	<p>logging file numbers <i>numbers</i></p> <p>Configures the number of files which logs are written into. The default value is 16.</p>
	<p>logging flash interval <i>seconds</i></p> <p>Configures the interval at which logs are written into log files. The default value is 3600.</p>
	<p>logging life-time level <i>level days</i></p> <p>Configures the storage time of log files.</p>
Configuring Syslog Filtering	<p> (Optional) It is used to enable the syslog filtering function.</p>
	<p>logging filter direction { all buffer file server terminal }</p> <p>Configures the log filtering direction.</p>
	<p>logging filter type { contains-only filter-only }</p> <p>Configures the log filtering mode.</p>
	<p>logging filter rule exact-match module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i></p> <p>Configures the exact-match filtering rule.</p>
	<p>logging filter rule single-match { level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i> }</p> <p>Configures the single-match filtering rule.</p>
Configuring Syslog Monitoring	<p> (Optional) It is used to configure parameters of the syslog monitoring function.</p>
	<p>logging userinfo</p> <p>Enables logging of login/exit attempts.</p>
	<p>logging userinfo command-log</p> <p>Enables logging of operations.</p>
Synchronizing User Input with Log Output	<p> (Optional) It is used to synchronize the user input with log output.</p>
	<p>logging synchronous</p> <p>Synchronizes user input with log output.</p>

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 [<i>message-type</i> [uptime datetime [msec] [year]]]
Parameter Description	<i>message-type</i> : 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	<p>By default, logs are displayed in the following format (default format):</p> <pre>*timestamp: %module-level-mnemonic: content</pre> <p>If the standard syslog format is enabled, logs are displayed in the following format:</p> <pre>timestamp %module-level-mnemonic: content</pre> <p>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.</p>
----------------------------	--

▾ Enabling the Private Syslog Format

Command	service private-syslog
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>By default, logs are displayed in the following format (default format):</p> <pre>*timestamp: %module-level-mnemonic: content</pre> <p>If the private syslog format is enabled, logs are displayed in the following format:</p> <pre>timestamp module-level-mnemonic: content</pre> <p>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.</p>

▾ Enabling the RFC5424 Syslog Format

Command	service log-format rfc5424
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>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.</p>

Configuration Example

▾ Enabling the RFC3164 Log Format

Scenario	<p>It is required to configure the timestamp format as follows:</p> <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> Configure the syslog format.
	<pre>Ruijie# configure terminal Ruijie(config)# no service log-format rfc5424 Ruijie(config)# service timestamps log datetime year msec Ruijie(config)# service timestamps debug datetime year msec Ruijie(config)# service sysname Ruijie(config)# service sequence-numbers</pre>
Verification	<p>After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format.</p> <ul style="list-style-type: none"> 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.
	<pre>Ruijie(config)#exit 001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console Ruijie#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</pre>

📌 Enabling the RFC5424 Log Format

Scenario	It is required to enable the RFC5424 format.
-----------------	--

Configuration Steps	<ul style="list-style-type: none"> Configure the syslog format.
	<pre>Ruijie# configure terminal Ruijie(config)# service log-format rfc5424</pre>
Verification	<p>Verify that new syslogs are displayed in the RFC5424 format.</p> <ul style="list-style-type: none"> 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.
	<pre>Ruijie(config)#exit <133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console Ruijie#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 Delay-send logging: 2641 message lines logged logging to 192.168.23.89 by tftp</pre>

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	N/A
Description	
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	N/A
Description	
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	<i>level</i> : 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 { <i>number</i> all <i>number</i> console { <i>number</i> all <i>number</i> } } [except [<i>severity</i>]]
Parameter Description	<p><i>number</i>: Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000.</p> <p>all: Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7.</p> <p>console: Indicates the number of logs displayed on the Console per second.</p> <p>except <i>severity</i>: 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.</p>
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: <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● Configure parameters for displaying syslogs on the Console. <pre>Ruijie# configure terminal Ruijie(config)# logging count Ruijie(config)# logging console informational Ruijie(config)# logging rate-limit console 50</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration.

```
Ruijie(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
  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	<i>level</i> : 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: <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● Configure parameters for displaying syslogs on the monitor terminal. <pre>Ruijie# configure terminal Ruijie(config)# logging monitor informational Ruijie(config)# line vty 0 4 Ruijie(config-line)# monitor</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration.

```
Ruijie#show logging config
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 memory buffer.

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 [<i>buffer-size</i>] [<i>level</i>]
Parameter	<i>buffer-size</i> : Indicates the size of the memory buffer.
Description	<i>level</i> : 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	<ul style="list-style-type: none"> Configure parameters for writing syslogs into the memory buffer.
	<pre>Ruijie# configure terminal Ruijie(config)# logging buffered 131072 informational</pre>
Verification	<ul style="list-style-type: none"> Run the show logging config command to display the configuration and recent syslogs.

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● Configure parameters for writing syslogs into the memory buffer.
	<pre>Ruijie# configure terminal Ruijie(config)# logging buffered 131072 informational</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration and recent syslogs.
	<pre>Ruijie#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 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: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console 001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console //Logs displayed are subject to the actual output of the show logging command.</pre>

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 { <i>ip-address</i> } [udp-port <i>port</i>] Or logging { <i>ip-address</i> } [udp-prot <i>port</i>]
Parameter	<i>ip-address</i> : Specifies the IP address of the host that receives logs.
Description	udp-port <i>port</i> : 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 Ruijie product.

▾ Configuring the Level of Logs Sent to the Log Server

Command	logging trap [<i>level</i>]
Parameter Description	<i>level</i> : 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 <i>facility-type</i>
Parameter Description	<i>facility-type</i> : 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] <i>interface-type interface-number</i>
Parameter Description	<i>interface-type</i> : Indicates the interface type. <i>interface-number</i> : 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 <i>ip-address</i> }
Parameter Description	ip <i>ip-address</i> : Specifies the source IPv4 address of logs sent to the IPv4 log server.
Command	Global configuration mode

Mode	
Configuration Usage	<p>By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs.</p> <p>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.</p>

Configuration Example

📌 Sending Syslogs to the Log Server

Scenario	<p>It is required to configure the function of sending syslogs to the log server as follows:</p> <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● Configure parameters for sending syslogs to the log server.
	<pre>Ruijie# configure terminal Ruijie(config)# logging server 10.1.1.100 Ruijie(config)# logging trap debugging Ruijie(config)# logging source interface Loopback 0</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration.

```
Ruijie#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

- Syslogs 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 } [<i>max-file-size</i>] [<i>level</i>]
Parameter Description	<p>flash: Indicates that log files will be stored on the extended Flash.</p> <p><i>filename:</i> Indicates the log file name, which does not contain a file name extension. The file name extension is always txt.</p> <p><i>max-file-size:</i> Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default value is 128 KB.</p> <p><i>level:</i> Indicates the level of logs that can be written into a log file.</p>
Command Mode	Global configuration mode
Configuration Usage	<p>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.</p> <p>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.</p> <p>After this command is configured, logs will be written into log files every hour. If you run the logging file 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.</p>

✚ Configuring the Number of Log Files

Command	logging file numbers <i>numbers</i>
Parameter Description	<i>numbers</i> : Indicates the number of log files. The value ranges from 2 to 32.
Command Mode	Global configuration mode
Configuration Usage	<p>This command is used to configure the number of log files.</p> <p>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.</p>

↘ Configuring the Interval at Which Logs Are Written into Log Files


Command	logging flash interval <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the interval at which logs are written into log files. The value ranges from 1 s to 51,840s.
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 <i>level days</i>
Parameter Description	<p><i>level</i>: Indicates the log level.</p> <p><i>days</i>: Indicates the storage time of log files. The unit is day. The storage time is not less than seven days.</p>
Command Mode	Global configuration mode
Configuration Usage	<p>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.</p> <p>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.</p> <p>If the log storage time is not configured, logs are stored based on the file size to ensure compatibility with old configuration commands.</p>

↘ Immediately Writing Logs in the Buffer into Log Files

Command	logging flash flush
Parameter	N/A

Description	
Command Mode	Global configuration mode
Configuration Usage	<p>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.</p> <p> 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.</p>

Configuration Example

Writing Syslogs into Log Files

Scenario	<p>It is required to configure the function of writing syslogs into log files as follows:</p> <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● Configure parameters for writing syslogs into log files.
	<pre>Ruijie# configure terminal Ruijie(config)# logging file flash:syslog debugging Ruijie(config)# logging flash interval 600</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration.

```
Ruijie(config)#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 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	all: Filters out all logs.
Description	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 <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i> single-match { level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i> } }
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 <i>module-name</i>: Indicates the module name. Logs of this module will be filtered out. mnemonic <i>mnemonic-name</i>: Indicates the mnemonic. Logs with this mnemonic will be filtered out. level <i>level</i>: Indicates the log level. Logs of this level will be filtered out.

Command Mode	Global configuration mode
Configuration Usage	<p>Log filtering rules include exact-match and single-match.</p> <p>The no logging filter rule exact-match [module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i>] 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.</p> <p>The no logging filter rule single-match [level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i>] 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.</p>

Configuration Example

Configuring Syslog Filtering

Scenario	<p>It is required to configure the syslog filtering function as follows:</p> <ol style="list-style-type: none"> 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	<ul style="list-style-type: none"> ● Configure the syslog filtering function.
	<pre>Ruijie# configure terminal Ruijie(config)# logging filter direction server Ruijie(config)# logging filter direction terminal Ruijie(config)# logging filter type filter-only Ruijie(config)# logging filter rule single-match module SYS</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	<pre>Ruijie#configure Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#exit Ruijie# Ruijie#show running-config include logging logging filter direction server logging filter direction terminal logging filter rule single-match module SYS</pre>

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.

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 does not generate 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 does not generate logs when users modify device configurations.

Configuration Example

Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: <ol style="list-style-type: none"> 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog monitoring function.
	<pre>Ruijie# configure terminal Ruijie(config)# logging userinfo Ruijie(config)# logging userinfo command-log</pre>
Verification	<ul style="list-style-type: none"> ● 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.
	<pre>Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#interface GigabitEthernet 0/1 *Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface GigabitEthernet 0/1 Ruijie#show running-config include logging logging userinfo command-log</pre>

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	<ul style="list-style-type: none"> ● Configure the synchronization function. <pre>Ruijie# configure terminal Ruijie(config)# line console 0 Ruijie(config-line)# logging synchronous</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config begin line command to display the configuration.

```
Ruijie#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.

```
Ruijie(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
```

```
Ruijie(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 CWMP

7.1 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

7.2 Applications

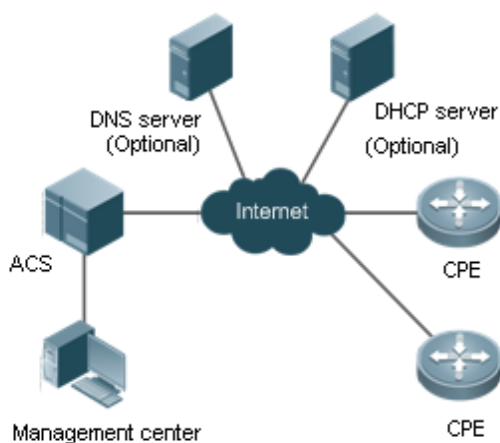
Typical Application	Scenario
CWMP Network Application Scenario	Initiate CPE-ACS connection, so as to upgrade the CPE firmware, upload the configuration files, restore the configuration, and realize other features.

7.2.1 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	<ul style="list-style-type: none"> ● 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 resolve the names.
-------------	---

Functional Deployment

HTTP runs on both CPEs and the ACS.

7.3 Features

Basic Concept

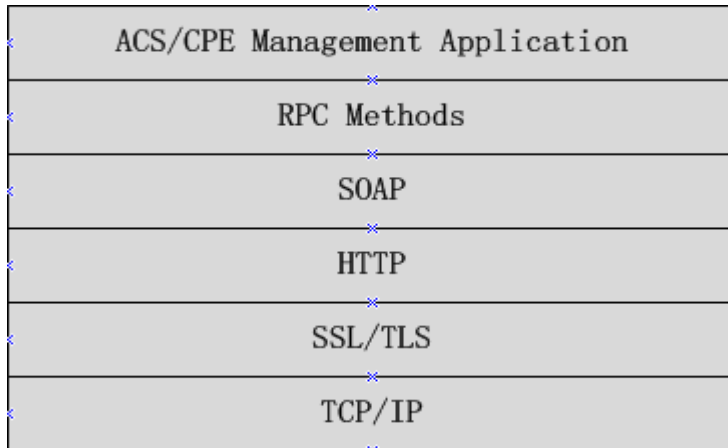
Major Terminologies

- **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.

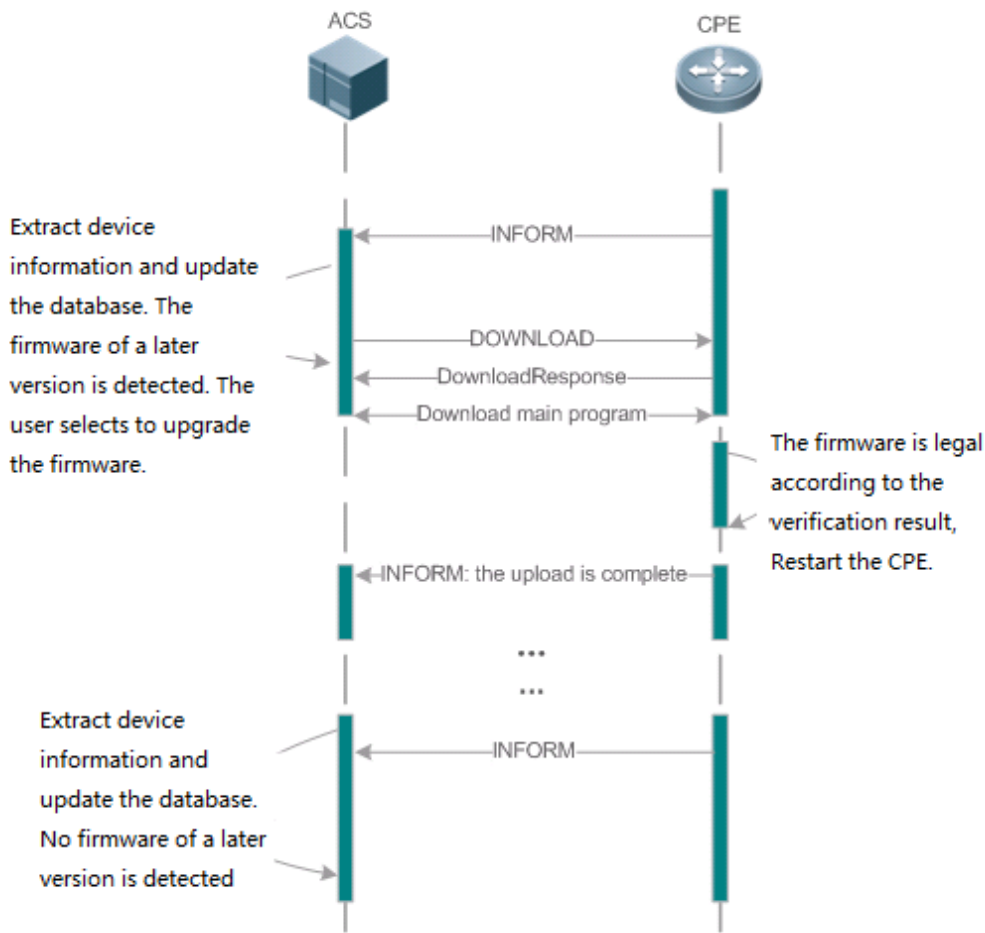
7.3.1 Upgrading the Firmware

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.

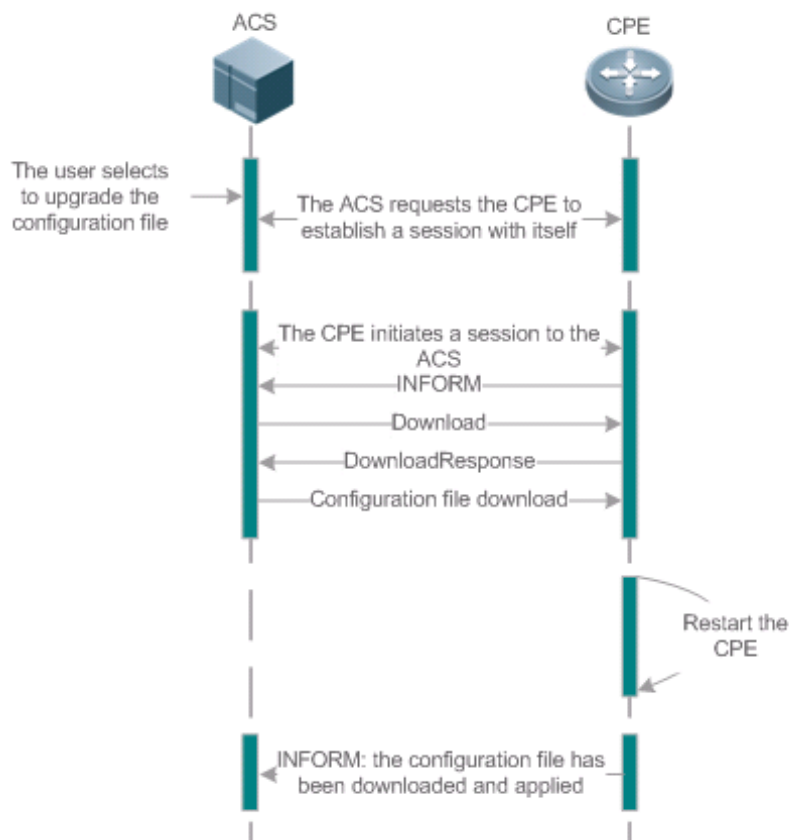
i The file server can be ACS or separately deployed.

7.3.2 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.

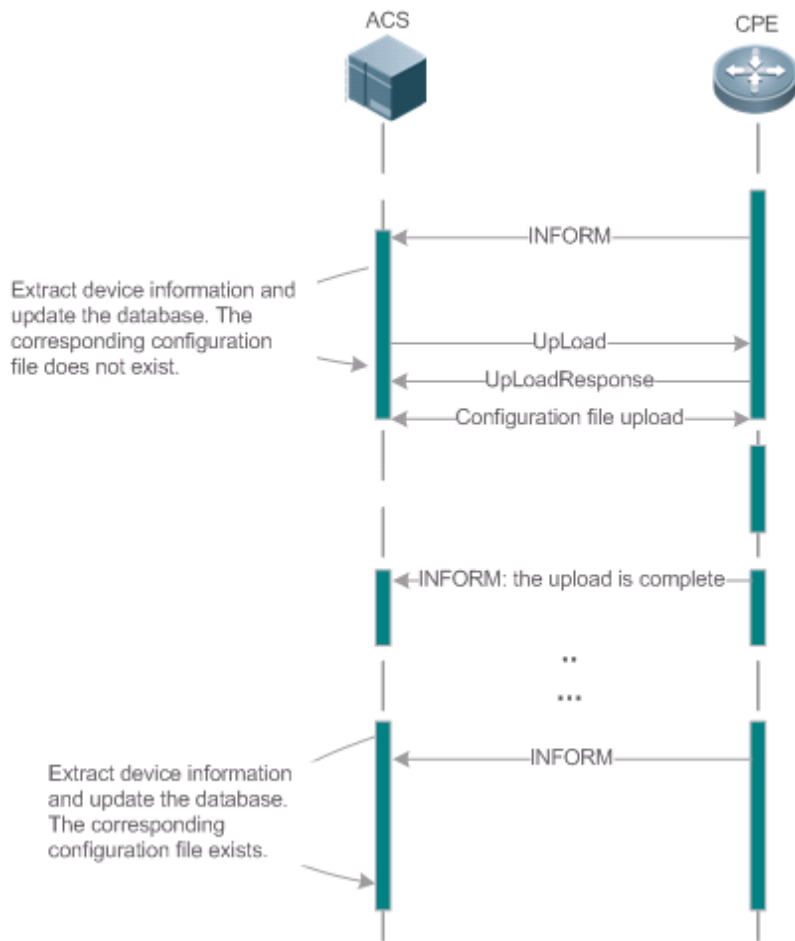
i The file server can be ACS or separately deployed.

7.3.3 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.

7.3.4 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.

7.4 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.

7.4.1 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	N/A
Description	
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 <i>username</i>
Parameter	username <i>username</i> : The ACS username for CWMP connection
Description	
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 { <i>password</i> <i>encryption-type</i> <i>encrypted-password</i> }
Parameter	<i>password</i> : ACS password
Description	<i>encryption-type</i> : 0 (no encryption) or 7 (simple encryption) <i>encrypted-password</i> : Password text
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 <i>username</i>
Parameter	<i>username</i> : CPE username
Description	
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 { <i>password</i> <i>encryption-type</i> <i>encrypted-password</i> }
Parameter	<i>password</i> : CPE password
Description	<i>encryption-type</i> : 0 (no encryption) or 7 (simple encryption) <i>encrypted-password</i> : Password text
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: <ul style="list-style-type: none"> ● 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
Parameter	<i>url</i> : ACS URL
Description	
Command Mode	CWMP configuration mode
Usage Guide	<p>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:</p> <ul style="list-style-type: none"> ● Be in format of http://host[:port]/path or https://host[:port]/path. ● Contain 256 characters at most.

↘ **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	<i>url</i> : CPE URL
Description	
Command Mode	CWMP configuration mode
Usage Guide	<p>If CPE URL is not configured, it is obtained through DHCP. The CPE URL must:</p> <ul style="list-style-type: none"> ● Be in format of http://ip [: port]/. ● Contain 256 characters at most.

Configuration Examples

i The following configuration examples describe CWMP-related configuration only.

↘ **Configuring Usernames and Passwords on the CPE**

Network Environment Figure 7-6	 <p>The diagram shows a server icon labeled 'ACS' connected to a cloud icon labeled 'Internet', which is then connected to a router icon labeled 'CPE'.</p>
Configuration Method	<ul style="list-style-type: none"> ● 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	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z.</pre>

	<pre>Ruijie(config)# cwmp Ruijie(config-cwmp)# acs username USERB Ruijie(config-cwmp)# acs password PASSWORDB Ruijie(config-cwmp)# cpe username USERB Ruijie(config-cwmp)# cpe password PASSWORDB</pre>
Verification	<ul style="list-style-type: none"> Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie # 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 : *****</pre>

Configuring the URLs of the ACS and the CPE

Network Environment	See Figure 7-6.
Configuration Method	<ul style="list-style-type: none"> Configure the ACS URL. Configure the CPE URL.
CPE	<pre>Ruijie# configure terminal Ruijie(config)# cwmp Ruijie(config-cwmp)# acs url http://10.10.10.1:7547/acs Ruijie(config-cwmp)# cpe url http://10.10.10.1:7547/</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie #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/</pre>

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 126 characters.
- The user-input plaintext password contains illegal characters.
- The URL of the ACS is set to **NULL**.
- The URL of the CPE is set to **NULL**.

7.4.2 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 <i>seconds</i>] [starttime <i>time</i>]
Parameter Description	<i>seconds</i> : Specifies the periodical notification interval of the CPE. The value range is from 30 to 3,600 in seconds. <i>time</i> : Specifies the date and time for starting periodical notification in <i>yyyy-mm-ddThh:mm:ss</i> format.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the periodic notification function of the CPE. <ul style="list-style-type: none"> 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
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of downloading main program and configuration files from the ACS. <ul style="list-style-type: none"> 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
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

↘ Disabling STUN port adaptation

- (Optional) Use this command to disable STUN port adaptation.
- STUN port adaptation is disabled by default.

Command	disable stun port-adaptive
Parameter Description	port-adaptive: Indicates STUN port adaptation.
Command Mode	CWMP configuration mode
Usage Guide	N/A

↘ 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	<i>seconds:</i> Specifies the delay for backup and restoration of the firmware and configuration file of the CPE.
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	<i>seconds:</i> Specifies the timeout period in seconds. The value range is from 10 to 600.

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	<p>The following example displays the CWMP configuration.</p> <pre>Ruijie(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 : ruijie 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</pre>

Configuration Examples

Configuring the Periodical Notification Interval of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval of the CPE to 60 seconds.
CPE	<pre>Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)#cpe inform interval 60</pre>

Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie #show cwmp configuration CWMP Status : enable CPE inform interval : 60s</pre>

↘ Disabling the Function of Downloading Firmware and Configuration Files from the ACS

Network Environment	See Figure 7-6.
Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Disable the function of downloading firmware and configuration files from the ACS.
CPE	<pre>Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)#disable download</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie #show cwmp configuration CWMP Status : enable CPE download status : disable</pre>

↘ Disabling the Function of Uploading Configuration and Log Files to the ACS

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Disable the CPE's function of uploading configuration and log files to the ACS.
CPE	<pre>Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)# disable upload</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie #show cwmp configuration CWMP Status : enable CPE upload status : disable</pre>

↘ Configuring the Backup and Restoration Delay

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 30 seconds.
CPE	<pre>Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)# cpe back-up Seconds 30</pre>
Verification	<ul style="list-style-type: none"> ● Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie #show cwmp configuration CWMP Status : enable CPE back up delay time : 30s</pre>

↘ Configuring the ACS Response Timeout of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Set the response timeout of the CPE to 30 seconds.
CPE	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# cwmp Ruijie(config-cwmp)# timer cpe-timeout 100</pre>
Verification	<ul style="list-style-type: none"> ● Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>Ruijie#show cwmp configuration CWMP Status : enable CPE wait timeout : 100s</pre>

Common Errors

N/A

7.5 Monitoring

Displaying

Description	Command
-------------	---------

Displays the CWMP configuration.	show cwmp configuration
Displays the CWMP running status.	show cwmp status

8 Configuring PoE

8.1 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

8.2 Applications

Application	Description
PoE Power Supply Scenario	In the scenario, a PoE switch powers powered devices (PDs) and implements data exchange.

8.2.1 PoE Power Supply Scenario

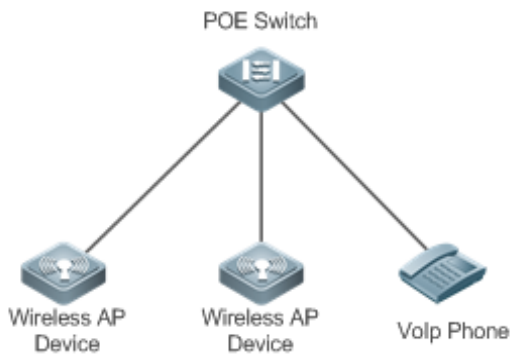
Scenario

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 8-1



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 disabled by default.

8.3 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 of Ruijie 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. Ruijie 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.
LLDP Classification	PDs can dynamically adjust allocated power by exchanging LLDP packets with PSE.

8.3.1 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 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.

Ruijie 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 auto.

You can run the **poe mode { auto | energy-saving }** 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 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.

8.3.2 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.

Ruijie provides PoE compatibility command to support compatibility with non-standard PoE devices.

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 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 PD Devices**

Non-standard PD compatibility is disabled by default.

Run the **poe legacy** command to configure compatibility with non-standard PD devices.

8.3.3 Auxiliary PoE Power Supply Functions

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 99.

You can run the **poewarning-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 **poenotification-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 **poepd-description pd-name** command to configure the PD descriptor for the port.

8.3.4 LLDP Classification

Working Principle

According to the IEEE 802.3at standard, PDs supporting 802.3at must support both secondary hardware classification (which is 2-Event Physical Layer classification in the standard) and LLDP classification (which is Data Link Layer classification in the standard). A PD can identify itself as a Class4 type by exchanging LLDP packets with the PSE. The PSE needs to support only one classification. Ruijie switches support LLDP classification.

After a PD of Class4 and Type2 is inserted into a PoE switch, the PoE switch performs detection and classification first and then supplies power for the PD. The PoE switch identifies a device as Type1 device and provides a maximum of 13 W power by default. After LLDP classification is performed, a PD can be identified as a Type2 device. If the PoE switch has sufficient power, the PD can obtain a maximum of 25.5 W power. If the PoE switch cannot allocate more power any longer, the PD will constantly send LLDP power request packets to request for power allocation.

The following table lists the maximum power that can be requested by PDs of each class.

Class	Type	Maximum Power (W)	Allocated Power (W)
Class 0	Type 1	13	15.4
Class 1	Type 1	3.9	4
Class 2	Type 1	6.5	7
Class 3	Type 1	13	15.4
Class 4	Type 1	13	15.4
Class 4	Type 2	25.5	30

Since the cable loss needs to be deducted from the power provided by the PSE, the allocated power is slightly higher than the maximum power requested by the PD.

This function is enabled by default and takes effect only in the auto mode.

Related Configuration

▾ Configuring LLDP Classification

By default, the system disables the LLDP classification.

You can run the **poe class-lldp enable** command to enable LLDP classification.

8.3.5 Auto Checking for PD

Working Principle

If ARP requests are sent to PD equipment periodically but no response is received for several times, it can be judged that PD equipment is not working. When the device detects that the PD device is offline, it will send a trap notification by default; if the **reboot-remote-pd** option is configured, the device will automatically reboot the PD device.





Related Configuration

↳ [Configuring Auto Checking](#)

By default, the system disables auto checking.

You can run the **poe auto-checking** command to enable auto checking.

8.4 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.
	poe uninterruptible-power	Configures uninterruptible power supply during hot startup.
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.
Configuring Auxiliary PoE Power Supply Functions	 (Optional) It is used to facilitate 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.
Enabling the LLDP	poe pd-description	Configures the PD descriptor of a port.
	 (Optional) It is used to manage the LLDP classification between the PoE and PDs.	

Configuration	Description and Command	
Classification	poe class-lldp enable	Uses the LLDP classification.
Configuring PoE Auto-checking	poe auto-checking pd-address	Configures the IP of PD device.
	poe auto-checking interval-time	Configures the detection interval of PoE auto-checking.
	poe auto-checking retry-time	Configures the retry times for one PoE auto-checking.
	poe auto-checking failure-action	Configures the action after detecting that the PD is offline.
	poe auto-checking reboot-time	Configures the reboot waiting time of PoE auto-checking.
	poe auto-checking	Enables PoE auto-checking.

8.4.1 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.
- Configure **reserve-power** to reserve 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 auto 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.
- 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.
- Support the global configuration.

↘ **Configuring Reserve Power**

↘ (Optional) Run the **energy-saving** command to configure reserve power.

- This function takes effect only when the switch works in energy-saving mode.
- If you configure reserve power in energy-saving mode, the ports already powered on may be powered off.

↘ **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. If you forget to save the configuration, a prompt message will be displayed.
- 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	<code>poe mode { auto energy-saving }</code>
Parameter Description	{ auto energy-saving }: Indicates the auto, and energy-saving.
Command Mode	Global configuration mode
Usage Guide	-

▾ Configuring Uninterruptible Power Supply During Hot Startup

Command	<code>poe uninterruptible-power</code>
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration

Example

▾ Configuring the Power Supply Management Policies for the System

Scenario	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Switch the mode to the energy-saving mode. ● Set the reserve power to 20%. ● Support uninterruptible power supply during hot startup.
	<pre>Ruijie# configure terminal Ruijie(config)# poe mode energy-saving Ruijie(config)# poe uninterruptible-power Ruijie(config)# exit</pre>

	Ruijie# write
Verification	Run the show poe powersupply command to view the configurations and the power supply information.
	<pre> Ruijie#show poe powersupply Device member : 1 Power management : energy-saving PSE total power : 1000W PSE total power consumption : 369.6W PSE total remain power : 630.4W PSE total powered port : 0 PSE disconnect mode : dc PSE reserve power : 20% PSE warning power : 99% PSE class lldp : disable PSE member : 1 PSE Power Enabled : enable PSE max power : 369.6W PSE priority : low PSE alloc power : 369.6W PSE available power : 295.7W PSE total power consumption : 0 W PSE total remain power : 295.7W PSE peak power : 0 W PSE average power : 0 W PSE powered port : 0 </pre>

8.4.2 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.

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.
- This function is useless when the switch works in static mode because the power is allocated as configured by the user. If priority is configured before the switch works in static mode, the command will be displayed but does not take effect.
- Support the global configuration and port-based configuration.

▾ Configuring Compatibility with Non-standard PDs

- (Optional) It is disabled by default.
- If connected PDs do not meet the PoE standard, compatibility 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.
- The class of non-standard PoE devices is 0.
- If this command is not configured, non-standard PDs connected will not be powered on and the system will not display any prompt information.

- This function can be configured on a single port.

▾ 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, a port is powered off and not powered on again.
- The max-power for PoE switch supporting only 802.3af is in the range 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.

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 <i>name</i>
Parameter Description	<i>name</i> : 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	Interface configuration mode
Usage Guide	-

↘ Configuring the Maximum Power Allocated to a Port

Command	poe max-power int
Parameter Description	<i>Int</i> : Indicates the maximum power, ranging from 0 to 0-30 W. The value ranges from 0 to 15.4 for a system supporting only 802.3af.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration

Example

↘ Configuring the Power Supply Management Policies for a Port

Scenario	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.
	<pre>Ruijie# configure terminal Ruijie(config)# time-range poe-time Ruijie(config-time-range)# periodic daily 8:00 to 12:00 Ruijie(config-time-range)# exit Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if)# poe power-off time-range poe-time Ruijie(config-if)# poe priority critical Ruijie(config-if)# poe max-power 15.4</pre>
Verification	Run the show poe interface gigabitEthernet 0/1 command to view the configurations and the power supply information.
	<pre>Ruijie#show poe interface gigabitEthernet 0/1 Interface : gi0/1 Power enabled : enable Power status : on Max power : 15.4W</pre>

Allocate power	: N/A
Current power	: 14.8 W
Average power	: 14.8 W
Peak power	: 14.8 W
LLDP requested power	: 0 W
LLDP allocated power	: 0 W
Voltage	: 53.5 V
Current	: 278 mA
PD class	: 4
Trouble cause	: None
Priority	: critical
Legacy	: off
Power-off time-range	: poe-time
Power management	: auto

8.4.3 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 <i>int</i>
Parameter Description	<i>int</i> : 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 <i>pd-name</i>
Parameter Description	<i>pd-name</i> : 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
	<pre>Ruijie# configure terminal Ruijie(config)# poe poe warnig-power 80 Ruijie(config)# poe notification-control enable Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if)# poe pd-description ap220</pre>
Verification	Run the show running-config command to view the configurations and power supply information.

8.4.4 Enabling the LLDP Classification

Configuration Effect

- Configure **class-lldp** to support power supply and power negotiation through LLDP between a PoE switch and PDs.

Configuration Steps

▾ Using the LLDP Classification

- (Optional) It is disabled by default.
- The system switches to the auto mode. Enable the LLDP classification function in the global configuration mode and verify that there is no max-power configuration on the ports.
- If a power is configured with the **Max-power** command to restrict the maximum power, the LLDP power adjustment function of the port fails.
- A PoE switch does not allow PDs to adjust their priorities through LLDP requests. The port priorities are managed by the PoE switch in a unified manner.
- Support port-based configuration.

Verification

View the "PD class" information in the PoE information of a port to check whether the port is in the LLDP correlation with PDs.

Related Commands

Using the LLDP Classification

Command	poe class-lldp enable
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration

Example

Configuring the Power Supply Management Policies for a Port

Scenario	Correlate a PD of Class4 with the PSE.
Configuration Steps	Enable the LLDP classification.
	<pre>Ruijie# configure terminal Ruijie(config)# poe class-lldp enable</pre>
Verification	Run the show poe interface gigabitEthernet 0/1 command to view the configurations and the power supply information.
	<pre>Ruijie#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 : 0 W LLDP allocated power : 0 W Voltage : 53.5 V Current : 278 mA PD class : 4(Type1) Trouble cause : None</pre>

Priority	: critical
Legacy	: off
Power-off time-range	: poe-time
Power management	: auto

8.4.5 Configuring PoE Auto-checking

Configuration Effect

- After PoE auto-checking function is enabled, the system will perform automatic detection on the configured port. When it detects that the PD device is offline, it will send a trap notification by default; if the **reboot-remote-pd** option is configured, it will automatically reboot the PD device.

Configuration Steps

▾ Configuring the IP Address of PD Device

- (Mandatory) No PD address is configured by default.
- Configure the IP address of the PD device. On the SVI port, it supports configuration in batch, and need to specify the port where the PD device is connected.
- The IP address of the PD device can be configured on the Web or using CLI commands.
- Support the port-based configuration.

▾ Configuring PoE Auto-checking Detection Interval

- (Optional) 10s by default.
- Configure the detection interval of PoE auto-checking.
- The PoE auto-checking detection interval under this port can be configured on the Web or using CLI commands.
- Support the port-based configuration.

▾ Configuring PoE Auto-checking Detection Retry Times

- (Optional) 1 time by default.
- Configure the retry times for one round of PoE auto-checking.
- The PoE auto-checking detection retry times under this port can be configured on the Web or using CLI commands.
- Support the port-based configuration.

▾ Configuring PoE Auto-checking Detection Failure Action

- (Optional) It is configured as **nothing** by default.
- Configure the action after the PD is offline. **nothing** is to send a trap notification but take no action; **reboot-remote-pd** is to reboot the PD device.
- The PoE auto-checking detection failure action of the port can be configured on the Web or using CLI commands.
- Support the port-based configuration.

▾ Configuring PoE Auto-checking Reboot Waiting Time

- (Optional) 15s by default.
- When the PoE auto-checking detection failure action is configured as **reboot-remote-pd**, the waiting time is the time for device to detect the port again.
- The PoE auto-checking restart waiting time under this port can be configured on the Web or using CLI commands.
- Support the port-based configuration.

▾ Enabling PoE Auto-checking

- (Optional) It is disabled by default.
- Configure the PoE auto-checking on switch. After it is enabled, the PD device will be checked repeatedly.
- The PoE auto-checking switch can be configured on the Web or using CLI commands.
- Support the global configuration.

Verification

Run the **show poe auto-checking** command to check the relevant configuration of PoE auto-checking, enable the PoE auto-checking function, and check whether the system can detect the offline PD device, send trap notification, or automatically reboot the PD device.

Related Commands

▾ Configuring the IP Address of the PD Device

Command	poe auto-checking pd-address <i>ip-address interface interface-type interface-number</i>
Parameter Description	<i>ip-address</i> : 32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots. <i>interface-type</i> : Specifies interface type. <i>interface-number</i> : Specifies interface number.
Command Mode	Interface configuration mode
Usage Guide	N/A

▾ Configuring PoE Auto-checking Detection Interval

Command	poe auto-checking interval-time <i>interval</i>
Parameter Description	<i>interval</i> : The detection interval of PoE auto-checking, in the range from 10 to 120.
Command Mode	Interface configuration mode
Usage Guide	N/A

▾ Configuring PoE Auto-checking Detection Retry Times

Command	poe auto-checking retry-time <i>int</i>
Parameter Description	<i>int</i> : Detection retry times, in the range from 1 to 5.
Command	Interface configuration mode

Mode	
Usage Guide	N/A

▾ Configuring PoE Auto-checking Detection Failure Action

Command	poe auto-checking failure-action [nothing reboot-remote-pd]
Parameter Description	[nothing reboot-remote-pd]: The action after detecting the PD is offline. nothing is to send a trap notification but take no action; reboot-remote-pd is to reboot the PD device.
Command Mode	Interface configuration mode
Usage Guide	N/A

▾ Configuring PoE Auto-checking Reboot Waiting Time

Command	poe auto-checking reboot-time interval
Parameter Description	<i>interval</i> : The reboot waiting time of PoE auto-checking, in the range from 10 to 120.
Command Mode	Interface configuration mode
Usage Guide	N/A

▾ Enabling PoE Auto-checking

Command	poe auto-checking
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

▾ Configuring PoE Auto-checking Function.

Scenario	<ul style="list-style-type: none"> ● There are several PD devices connected with the switch, and require online test. ● When a PD device is offline, it is necessary to automatically reboot it in addition to sending a trap notification. ● The detection interval is 15s. ● The retry times is 3. ● The waiting time for reboot is 20s.
Configuration Steps	<ul style="list-style-type: none"> ● Configure the IP address of PD for PoE auto-checking. ● Configure the action after PD is offline as reboot-remote-pd. ● Configure detection parameter of PoE auto-checking. ● Enable the PoE auto-checking on switch.

	<pre> Ruijie# configure terminal Ruijie(config-vlan)#int vlan 2 Ruijie(config-if-VLAN 2)#ip address 192.168.1.1/24 Ruijie(config-if-VLAN 2)#poe auto-checking pd-address 192.168.1.2 interface gi0/1 Ruijie(config-if-VLAN 2)#poe auto-checking pd-address 192.168.1.3 interface gi0/2 Ruijie(config-if-VLAN 2)#poe auto-checking failure-action reboot-remote-pd Ruijie(config-if-VLAN 2)#poe auto-checking interval-time 15 Ruijie(config-if-VLAN 2)#poe auto-checking retry-time 3 Ruijie(config-if-VLAN 2)#poe auto-checking reboot-time 20 Ruijie(config)#poe auto-checking </pre>
Verification	Run the show poe auto-checking command to view the PoE auto-checking configurations and run the show poe auto-checking status command to view the PoE auto-checking status.

8.5 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
Displays the auto-checking configuration and status of all ports.	show poe auto-checking

Ethernet Switching Configuration

1. Configuring Interfaces
2. Configuring MAC Addresses
3. Configuring Aggregated Port
4. Configuring VLAN
5. Configuring MAC VLAN
6. Configuring Protocol VLAN
7. Configuring Private VLAN
8. Configuring Voice VLAN
9. Configuring VLAN Mapping
10. Configuring STP/RSTP/MSTP
11. Configuring LLDP

1 Configuring Interfaces

1.1 Overview

Interfaces are important in implementing data switching on network devices. Ruijie devices support two types of interfaces: physical ports and logical interfaces. A physical port is a hardware port on a device, such as the 100M Ethernet interface and gigabit Ethernet interface. A logical interface 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.

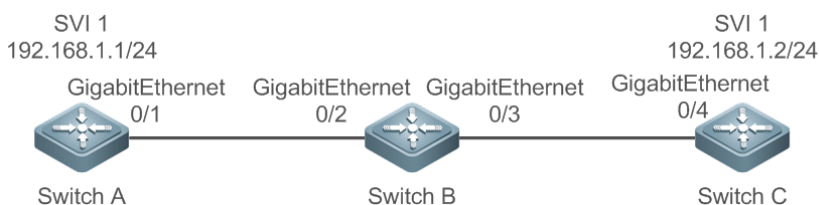
1.2 Applications

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.

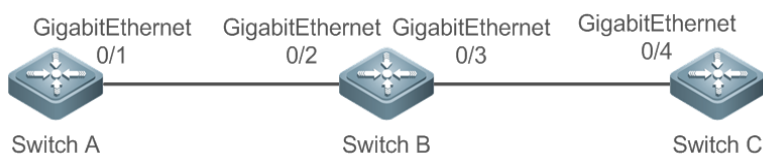
Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 0/1 and GigabitEthernet 0/2.
- Connect Switch B to Switch C through physical ports GigabitEthernet 0/3 and GigabitEthernet 0/4.
- Configure GigabitEthernet 0/1, GigabitEthernet 0/2, GigabitEthernet 0/3, and GigabitEthernet 0/4 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 0/1 and GigabitEthernet 0/2.
- Connect Switch B to Switch C through physical ports GigabitEthernet 0/3 and GigabitEthernet 0/4.
- Configure GigabitEthernet 0/1, GigabitEthernet 0/2, GigabitEthernet 0/3, and GigabitEthernet 0/4 as L3 routed ports.
- Configure IP addresses from a network segment for GigabitEthernet 0/1 and GigabitEthernet 0/2. The IP address of GigabitEthernet 0/1 is 192.168.1.1/24, and the IP address of GigabitEthernet 0/2 is 192.168.1.2/24.
- Configure IP addresses from a network segment for GigabitEthernet 0/3 and GigabitEthernet 0/4. The IP address of GigabitEthernet 0/3 is 192.168.2.1/24, and the IP address of GigabitEthernet 0/4 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.
- 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 Ruijie devices fall into three categories:

- L2 interface
 - L3 interface (supported by L3 devices)
 - Fiber channel (FC) interface (supported by some data center products)
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
3. FC interfaces are classified into the following types:
- FC interface
 - FC AP port

↘ **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.

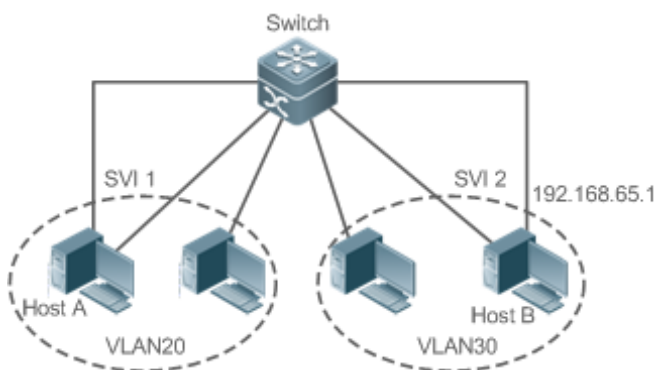
For L2 switching, an AP port is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP port are balanced among the L2 AP member ports. If one member link fails, the L2 AP port automatically transfers the traffic on the faulty 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.

- i** 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.

↘ FC Interface

The FC interface is a physical port used to support communication between the FC storage area networks (SANs). You can configure different working modes (E, F, or NP) for the FC interface to set up connections with the existing or a newly-created FC SAN, thus implementing networking.

↘ FC AP Port

The FC AP port is similar to a L2 or L3 AP port. The FC AP port is a virtual logical port that binds multiple FC physical ports that work in E mode. Theoretically, the bandwidth of an FC AP port is equal to the sum of the bandwidths of all member ports. Therefore, the FC aggregation function can meet the requirement for a higher bandwidth.

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.
Bandwidth	You can configure the bandwidth of an interface.
Load Interval	You can specify the interval for load calculation of an interface.

Feature	Description
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.
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.
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

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. If the device supports VSU or 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.

This device supports the stand-alone mode only.

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.

You can select fiber or copper as the medium of a combo port. Regardless of the medium selected, the combo port uses the same port ID.

The ID of an AP 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 0/1 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 lose 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 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.

1.3.4 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.

1.3.5 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.

1.3.6 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.

1.3.7 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.

1.3.8 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.

1.3.9 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.

1.3.10 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.)

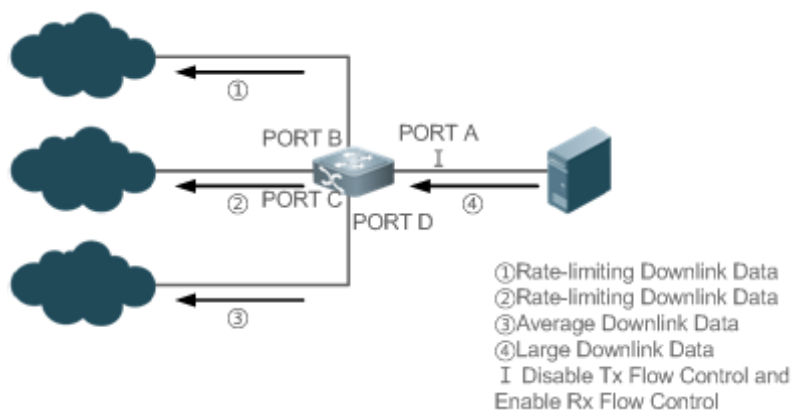
↘ Flow Control

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.

1.3.11 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.

1.3.12 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.

1.3.13 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.

1.3.14 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.

1.3.15 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 detects flapping every 2s or 10s. If flapping occurs six times within 2s on a port, the device displays a prompt. If 10 prompts are displayed continuously, that is, port flapping is detected continuously within 20s, the port is disabled. If flapping occurs 10 times within 10s on a port, the device displays a prompt without disabling the port.


1.3.16 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.

1.4 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.
	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.	

Configuration	Description and Command	
	logging [link-updown error-frame link-dither]	Configures the syslog function on an interface in global configuration mode.
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.
	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.
	errdisable recovery	Recovers a port in errdisable state in global configuration mode.
eee enable	Enables EEE in interface 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.

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 <i>interface-type interface-number</i>
Parameter Description	<i>interface-type interface-number</i> : 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 Mode	Global configuration mode
Usage Guide	<ul style="list-style-type: none"> ● 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 { <i>port-range</i> macro <i>macro_name</i> }
Parameter Description	<i>port-range</i> : Indicates the type and ID range of interfaces. These interfaces can be Ethernet physical ports, AP ports, SVIs, or loopback interfaces. <i>macro_name</i> : Indicates the name of the interface range macro.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	<ul style="list-style-type: none"> ● 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 <i>macro_name</i> 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 <i>string</i>
Parameter Description	<i>string</i> : 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**

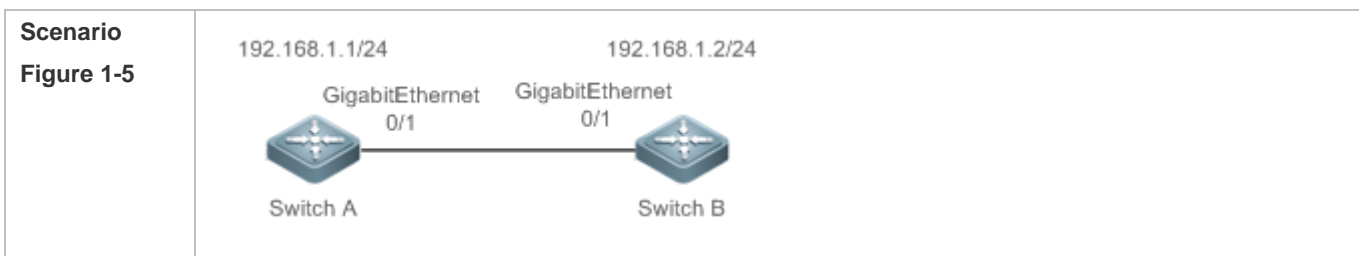
- Run the **physical-port dither protect** command in global configuration mode. Frequently remove and insert the network cable on a physical port to simulate port flapping. Verify that a syslog indicating port flapping is displayed on the Console. After such a syslog is displayed for several times, 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**



<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>A</p>	<pre>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</pre>
<p>B</p>	<pre>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</pre>
<p>Verification</p>	<p>Perform verification on Switch A and Switch B as follows:</p> <ul style="list-style-type: none"> ● Run the shutdown command on port GigabitEthernet 0/1, and check whether GigabitEthernet 0/1 and SVI 1 are Down. ● Run the shutdown command on port GigabitEthernet 0/1, and check whether a trap indicating that this interface is Down is sent. ● Restart the device, and check whether the index of GigabitEthernet 0/1 is the same as that before the restart.
<p>A</p>	<pre>A# show interfaces gigabitEthernet 0/1</pre>

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

	<p>0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort</p> <p>4 packets output, 408 bytes, 0 underruns, 0 dropped</p> <p>0 output errors, 0 collisions, 0 interface resets</p> <p>A# show interfaces vlan 1</p> <p>Index(dec):4097 (hex):1001</p> <p>VLAN 1 is UP, line protocol is DOWN</p> <p>Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)</p> <p>Interface address is: 192.168.1.1/24</p> <p>ARP type: ARPA, ARP Timeout: 3600 seconds</p> <p>MTU 1500 bytes, BW 1000000 Kbit</p> <p>Encapsulation protocol is Ethernet-II, loopback not set</p> <p>Keepalive interval is 10 sec, set</p> <p>Carrier delay is 2 sec</p> <p>Rxload is 0/255, Txload is 0/255</p>																																													
<p>B</p>	<p>B# show interfaces gigabitEthernet 0/1</p> <p>Index(dec):1 (hex):1</p> <p>GigabitEthernet 0/1 is administratively down, line protocol is DOWN</p> <p>Hardware is GigabitEthernet</p> <p>Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b)</p> <p>MTU 1500 bytes, BW 1000000 Kbit</p> <p>Encapsulation protocol is Bridge, loopback not set</p> <p>Keepalive interval is 10 sec, set</p> <p>Carrier delay is 2 sec</p> <p>Rxload is 1/255, Txload is 1/255</p> <table border="1" data-bbox="363 1496 1406 1962"> <thead> <tr> <th>Queue</th> <th>Transmitted packets</th> <th>Transmitted bytes</th> <th>Dropped packets</th> <th>Dropped bytes</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>3</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>4</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>6</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>7</td> <td>4</td> <td>440</td> <td>0</td> <td>0</td> </tr> </tbody> </table> <p>Switchport attributes:</p>	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
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																																										

```
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 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	Interface configuration mode

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 Bandwidth of an Interface

- Optional.
- Generally, the bandwidth of an interface is the same as the speed of the interface.

Command	bandwidth <i>kilobits</i>
Parameter Description	<i>kilobits:</i> 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] <i>num</i> up [milliseconds] <i>num</i> }
Parameter Description	<i>num:</i> 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.
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 <i>seconds</i>
Parameter Description	<i>seconds</i> : 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

▾ 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 <i>time</i>]
Parameter Description	<i>time</i> : 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 EEE

- Optional.
- The EEE mode of a port is enabled after this command is configured.

Command	eee enable
Parameter Description	N/A
Command	Interface configuration mode

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 [<i>interface-type interface-number</i>] [description switchport trunk]
Parameter	<i>interface-type interface-number</i> : Indicates the type and number of the interface.
Description	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.
	<pre>A#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 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 Active vlan lists:1, 3-4 Queueing strategy: FIFO Output queue 0/0, 0 drops; Input queue 0/75, 0 drops</pre>

```
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	<i>interface-type interface-number</i> : Indicates the type and number of an interface.
Description	status : Indicates the EEE status of 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.

```
Ruijie#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.

```
Ruijie#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

Configuration Example

Configuring Interface Attributes

<p>Scenario Figure 1-6</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> 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.
<p>A</p>	<pre>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</pre>

	<pre>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</pre>
B	<pre>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</pre>
C	<pre>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</pre>
D	<pre>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</pre>

	<pre>A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2</pre>
<p>Verification</p>	<p>Perform verification on Switch A, Switch B, Switch C, and Switch D as follows:</p> <ul style="list-style-type: none"> ● 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.
<p>A</p>	<pre>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</pre>

	<p>363 packets output, 82260 bytes, 0 underruns, 0 dropped</p> <p>0 output errors, 0 collisions, 0 interface resets</p>
<p>B</p>	<pre> 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 </pre>

<p>C</p>	<pre> 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 </pre>
<p>D</p>	<pre> 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 </pre>

	<p>Keepalive interval is 10 sec, set</p> <p>Carrier delay is 2 sec</p> <p>Ethernet attributes:</p> <p style="padding-left: 20px;">Last link state change time: 2012-12-22 14:00:48</p> <p style="padding-left: 20px;">Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds</p> <p style="padding-left: 20px;">Priority is 0</p> <p style="padding-left: 20px;">Admin medium-type is Copper, oper medium-type is Copper</p> <p style="padding-left: 20px;">Admin duplex mode is AUTO, oper duplex is Full</p> <p style="padding-left: 20px;">Admin speed is AUTO, oper speed is 100M</p> <p style="padding-left: 20px;">Flow control admin status is OFF, flow control oper status is OFF</p> <p style="padding-left: 20px;">Admin negotiation mode is OFF, oper negotiation state is ON</p> <p style="padding-left: 20px;">Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF</p> <p>Rxload is 1/255, Txload is 1/255</p> <p>10 seconds input rate 0 bits/sec, 0 packets/sec</p> <p>10 seconds output rate 67 bits/sec, 0 packets/sec</p> <p style="padding-left: 20px;">362 packets input, 87760 bytes, 0 no buffer, 0 dropped</p> <p style="padding-left: 20px;">Received 0 broadcasts, 0 runts, 0 giants</p> <p style="padding-left: 20px;">0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort</p> <p style="padding-left: 20px;">363 packets output, 82260 bytes, 0 underruns, 0 dropped</p> <p style="padding-left: 20px;">0 output errors, 0 collisions, 0 interface resets</p>
--	---

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 [<i>interface-type interface-number</i>]
Resets the interface hardware.	clear interface <i>interface-type interface-number</i>

Displaying

▾ Displaying Interface Configurations and Status

Description	Command
Displays all the status and configuration information of a specified interface.	show interfaces [<i>interface-type interface-number</i>]
Displays the interface status.	show interfaces [<i>interface-type interface-number</i>] status

Description	Command
Displays the interface errdisable status.	show interfaces [<i>interface-type interface-number</i>] status err-disable
Displays the link status change time and count of a specified port.	show interfaces [<i>interface-type interface-number</i>] link-state-change statistics
Displays the administrative and operational states of switch ports (non-routed ports).	show interfaces [<i>interface-type interface-number</i>] switchport
Displays the description and status of a specified interface.	show interfaces [<i>interface-type interface-number</i>] description
Displays the counters of a specified port, among which the displayed speed may have an error of $\pm 0.5\%$.	show interfaces [<i>interface-type interface-number</i>] counters
Displays the number of packets increased in a load interval.	show interfaces [<i>interface-type interface-number</i>] counters increment
Displays statistics about error packets.	show interfaces [<i>interface-type interface-number</i>] counters error
Displays the packet sending/receiving rate of an interface.	show interfaces [<i>interface-type interface-number</i>] counters rate
Displays a summary of interface information.	show interfaces [<i>interface-type interface-number</i>] 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 [<i>interface-type interface-number</i>] line-detect
Displays the bandwidth usage of an interface.	show interfaces [<i>interface-type interface-number</i>] usage
Displays the EEE status of an interface.	show eee interfaces [<i>interface-type interface-number</i>] status

Debugging



System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

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.

i 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

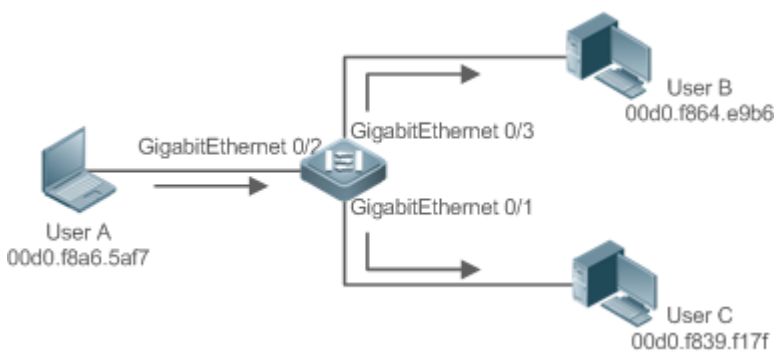


Figure 2-2 MAC Address Table 1

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

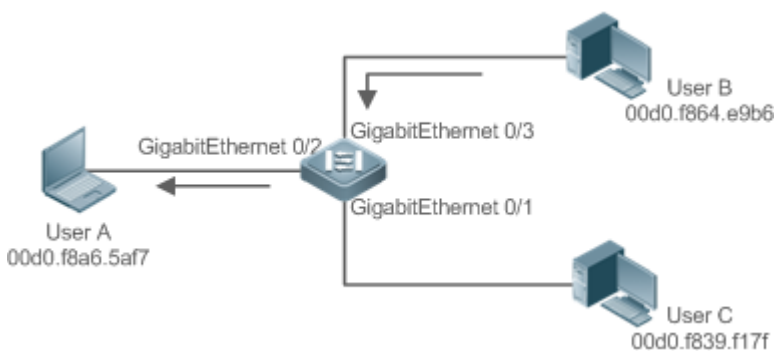


Figure 2-4 MAC Address Table 2

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

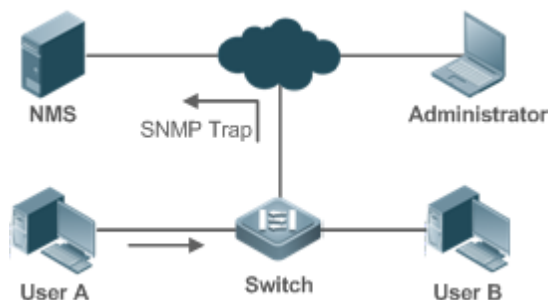
- With MAC address learning, a layer-2 switch forwards packets through unicast, reducing broadcast packets and network load.

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.

i 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.

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.

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	enable: Enables global MAC address learning.
Description	disable: Disable global MAC address learning.
Defaults	Global MAC address learning is enabled by default.
Command	Global configuration mode

Mode	
Usage Guide	N/A

- i** 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.

- i** 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 <i>value</i>
Parameter Description	<i>value</i> : Indicates the aging time. The value is either 0 or in the range from 10 to 630.
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.

- i** 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 <i>mac-address</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]																																																		
Parameter Description	address <i>mac-address</i> : Displays the information of a specific dynamic MAC address. interface <i>interface-id</i> : Specifies a physical interface or an AP port. vlan <i>vlan-id</i> : Displays the dynamic MAC addresses in a specific VLAN.																																																		
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																																																		
Usage Guide	N/A																																																		
	<pre>Ruijie# show mac-address-table dynamic</pre> <table border="1"> <thead> <tr> <th>Vlan</th> <th>MAC Address</th> <th>Type</th> <th>Interface</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0000.0000.0001</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:13:15</td> </tr> <tr> <td>1</td> <td>0001.960c.a740</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:13:16</td> </tr> <tr> <td>1</td> <td>0007.95c7.dff9</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:14:15</td> </tr> <tr> <td>1</td> <td>0007.95cf.eee0</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:15:20</td> </tr> <tr> <td>1</td> <td>0007.95cf.f41f</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:18:30</td> </tr> <tr> <td>1</td> <td>0009.b715.d400</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:20:55</td> </tr> <tr> <td>1</td> <td>0050.bade.63c4</td> <td>DYNAMIC</td> <td>gigabitethernet 0/1</td> <td>2020-12-09 8:23:18</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Field</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Vlan</td> <td>Indicates the VLAN where the MAC address resides.</td> </tr> <tr> <td>MAC Address</td> <td>Indicates a MAC Address.</td> </tr> <tr> <td>Type</td> <td>Indicates a MAC address type.</td> </tr> <tr> <td>Interface</td> <td>Indicates the interface where the MAC address resides.</td> </tr> </tbody> </table>	Vlan	MAC Address	Type	Interface	Time	1	0000.0000.0001	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:13:15	1	0001.960c.a740	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:13:16	1	0007.95c7.dff9	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:14:15	1	0007.95cf.eee0	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:15:20	1	0007.95cf.f41f	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:18:30	1	0009.b715.d400	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:20:55	1	0050.bade.63c4	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:23:18	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.
Vlan	MAC Address	Type	Interface	Time																																															
1	0000.0000.0001	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:13:15																																															
1	0001.960c.a740	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:13:16																																															
1	0007.95c7.dff9	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:14:15																																															
1	0007.95cf.eee0	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:15:20																																															
1	0007.95cf.f41f	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:18:30																																															
1	0009.b715.d400	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:20:55																																															
1	0050.bade.63c4	DYNAMIC	gigabitethernet 0/1	2020-12-09 8:23:18																																															
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
	<pre>Ruijie# show mac-address-table aging-time</pre> <p>Aging time: 300</p>

Configuration Example

Configuring Dynamic MAC Address

<p>Scenario Figure 2-6</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
	<pre>Ruijie# configure terminal Ruijie(config-if-GigabitEthernet 0/1)# mac-address-learning Ruijie(config-if-GigabitEthernet 0/1)# exit Ruijie(config)# mac aging-time 180 Ruijie# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Check MAC address learning on an interface. ● Display the aging time for dynamic MAC addresses. ● Display all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	<pre>Ruijie# show mac-address-learning GigabitEthernet 0/1 learning ability: enable Ruijie# show mac aging-time Aging time : 180 seconds Ruijie# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1 Vlan MAC Address Type Interface Time ----- 1 00d0.f800.1001 STATIC GigabitEthernet 0/1 2020-12-09 8:23:18</pre>

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 <i>mac-address</i> vlan <i>vlan-id</i> interface <i>interface-id</i>
Parameter	address <i>mac-address</i> : Specifies a MAC address.
Description	vlan <i>vlan-id</i> : Specifies a VLAN where the MAC address resides. interface <i>interface-id</i> : 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 <i>mac-address</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]
Parameter	address <i>mac-address</i> : Specifies a MAC address.
Description	interface <i>interface-id</i> : Specifies a physical interface or an AP port. vlan <i>vlan-id</i> : Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	<pre>Ruijie#show mac-address-table static Vlan MAC Address Type Interface Time ----- 1 00d0.f800.1001 STATIC GigabitEthernet 0/1 2020-12-10 8:13:15 1 00d0.f800.1002 STATIC GigabitEthernet 0/1 2020-12-10 8:15:47 1 00d0.f800.1003 STATIC GigabitEthernet 0/1 2020-12-10 8:20:00</pre>

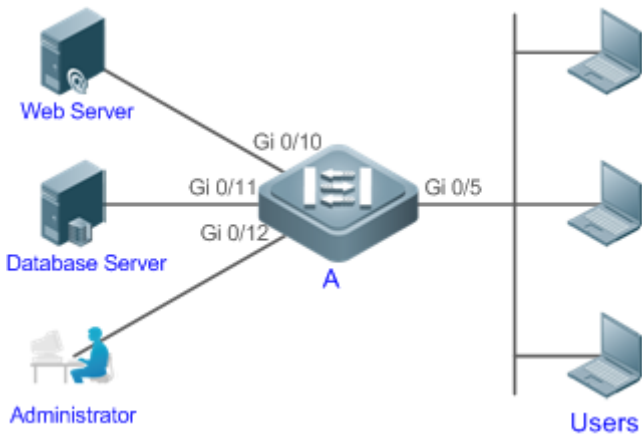
Configuration

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

<p>Scenario Figure 2-7</p>																					
<p>Configuration Steps</p>	<ul style="list-style-type: none"> Specify destination MAC addresses (<i>mac-address</i>). Specify the VLAN (<i>vlan-id</i>) where the MAC addresses reside. Specify interface IDs (<i>interface-id</i>). 																				
<p>A</p>	<pre>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</pre>																				
<p>Verification</p>	<p>Display the static MAC address configuration on a switch.</p>																				
<p>A</p>	<pre>A# show mac-address-table static</pre> <table border="1" data-bbox="331 1205 1362 1451"> <thead> <tr> <th>Vlan</th> <th>MAC Address</th> <th>Type</th> <th>Interface</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>00d0.f800.3232.0001</td> <td>STATIC</td> <td>GigabitEthernet 0/10</td> <td>2020-12-10 8:13:15</td> </tr> <tr> <td>2</td> <td>00d0.f800.3232.0002</td> <td>STATIC</td> <td>GigabitEthernet 0/11</td> <td>2020-12-10 8:15:47</td> </tr> <tr> <td>2</td> <td>00d0.f800.3232.1000</td> <td>STATIC</td> <td>GigabitEthernet 0/12</td> <td>2020-12-10 8:20:00</td> </tr> </tbody> </table>	Vlan	MAC Address	Type	Interface	Time	2	00d0.f800.3232.0001	STATIC	GigabitEthernet 0/10	2020-12-10 8:13:15	2	00d0.f800.3232.0002	STATIC	GigabitEthernet 0/11	2020-12-10 8:15:47	2	00d0.f800.3232.1000	STATIC	GigabitEthernet 0/12	2020-12-10 8:20:00
Vlan	MAC Address	Type	Interface	Time																	
2	00d0.f800.3232.0001	STATIC	GigabitEthernet 0/10	2020-12-10 8:13:15																	
2	00d0.f800.3232.0002	STATIC	GigabitEthernet 0/11	2020-12-10 8:15:47																	
2	00d0.f800.3232.1000	STATIC	GigabitEthernet 0/12	2020-12-10 8:20:00																	

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 <i>mac-address</i> vlan <i>vlan-id</i>
Parameter	address <i>mac-address</i> : Specifies a MAC address.
Description	vlan <i>vlan-id</i> : 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 <i>mac-address</i>] [vlan <i>vlan-id</i>]
Parameter	address <i>mac-address</i> : Specifies a MAC address.
Description	vlan <i>vlan-id</i> : Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	<pre>Ruijie#show mac-address-table filtering Vlan MAC Address Type Interface Time ----- 1 0000.2222.2222 FILTER 2020-12-09 9:16:33</pre>

Configuration

Example

Configuring a MAC Address for Packet Filtering

Configuration Steps	<ul style="list-style-type: none"> ● Specify a destination MAC address (<i>mac-address</i>) for filtering. ● Specify a VLAN where the MAC addresses resides.
	<pre>Ruijie# configure terminal Ruijie(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1</pre>
Verification	Display the filtered MAC address configuration.
	<pre>Ruijie# show mac-address-table filter Vlan MAC Address Type Interface Time ----- 1 00d0.f800.3232.0001 FILTER 2020-12-09 9:16:33</pre>

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 <i>host-addr</i> traps [version { 1 2c 3 [auth noauth priv] }] <i>community-string</i>
Parameter	host <i>host-addr</i>: Specifies the IP address of a receiver.
Description	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. <i>community-string</i>: 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	N/A
Description	
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	N/A
Description	

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 a MAC address is added. removed: Generates a notification when a 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 <i>value</i> history-size <i>value</i> }
Parameter Description	interval <i>value</i>: (Optional) Indicates the interval for generating MAC address change notifications. The value ranges from 1 to 3600 seconds,. history-size <i>value</i>: 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[<i>interface-id</i>]] history]
Parameter	Interface: Displays the configuration of MAC address change notification on all interfaces.

Description	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	<p>Display the configuration of global MAC address change notification.</p> <pre>Ruijie#show mac-address-table notification</pre> <p>MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 0</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Interval(Sec)</td> <td>Indicates the interval for generating MAC address change notifications.</td> </tr> <tr> <td>Maximum History Size</td> <td>Indicates the maximum number of entries in the table of notification history.</td> </tr> <tr> <td>Current History Size</td> <td>Indicates the current notification entry number.</td> </tr> </tbody> </table>	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.
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	<p>The figure shows an intranet of an enterprise. Users are connected to A via port Gi0/2.</p> <p>The Perform the configuration to achieve the following effects:</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Enable global MAC address change notification on A, and configure MAC address change notification on port Gi0/2.

	<ul style="list-style-type: none"> ● 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).
<p>A</p>	<pre>Ruijie# configure terminal Ruijie(config)# mac-address-table notification Ruijie(config)# interface gigabitEthernet 0/2 Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed Ruijie(config-if-GigabitEthernet 0/2)# exit Ruijie(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2 Ruijie(config)# snmp-server enable traps Ruijie(config)# mac-address-table notification interval 300</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● 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. ● Display the history of MAC address change notifications.
<p>A</p>	<pre>Ruijie# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 0 Ruijie# show mac-address-table notification interface GigabitEthernet 0/2 Interface MAC Added Trap MAC Removed Trap ----- GigabitEthernet 0/2 Enabled Enabled Ruijie# show mac-address-table interface GigabitEthernet 0/2 Vlan MAC Address Type Interface ----- 1 00d0.3232.0001 DYNAMIC GigabitEthernet 0/2 Ruijie# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 1 Ruijie# show mac-address-table notification history History Index : 0 Entry Timestamp: 221683</pre>

	MAC Changed Message : Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2
--	--

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 <i>mac-address</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]

Displaying

Description	Command
Displays the MAC address table.	show mac-address-table { dynamic static filter } [address <i>mac-address mac-address</i>] [interface <i>interface</i>] [interface <i>interface-id</i>] [vlan <i>vlan</i> vlan <i>vlan-id</i>]
Displays the aging time for dynamic MAC addresses.	show mac-address-table aging-time
Displays the number of MAC address entries in the address table.	show mac-address-table count [interface <i>interface-id</i> vlan <i>vlan-id</i>]
Displays all the MAC addresses on the specified interface including static and dynamic MAC address	show mac-address-table interface [<i>interface-id</i>] [vlan <i>vlan-id</i>]
Display the MAC address learning.	show mac-address-learning
Displays the configuration and history of MAC address change notifications.	show mac-address-table notification [interface [<i>interface-id</i>]] history]
Displays all MAC addresses of the specified VLAN.	show mac-address-table vlan [<i>vlan-id</i>]

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

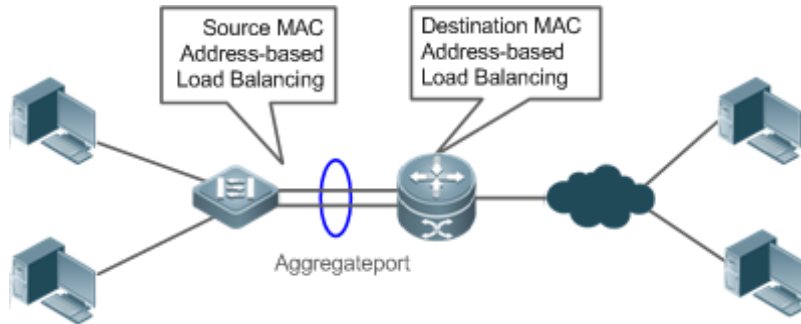
Applications	Description
AP Link Aggregation and Load Balancing	A large number of packets are transmitted between an aggregation device and a core device, which requires a greater bandwidth. To meet this requirement, you can bundle the physical links between the devices into one logical link to increase 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.

↘ AP Capacity Mode

The maximum number of member ports is fixed, which is equal to the maximum number of AP ports multiplied by the maximum number of member ports supported by a single AP port. If you want to increase the maximum number of AP ports, the maximum number of member ports supported by a single AP port must be reduced, and vice versa. This concerns the AP capacity mode concept. Some devices support the configuration of the AP capacity mode. For example, if the system supports 16,384 member ports, you can select the 1024 x 16, 512 x 32, and other AP capacity modes (Maximum number of AP ports multiplied by the maximum number of member ports supported by a single 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.

↳ Preferred AP Member Port

The preferred AP member port feature is used when an AP port is connected to a server with two systems. An AP member port is selected as the preferred port which will forward specified packets (packets of the management VLAN) to the server. These packets will not be distributed to other member ports by load balancing. This ensures the communication with the server.

 Configure the port connected to the management network interface card (NIC) of the server as the preferred AP member port.

Some Linux servers have two systems. For example, an HP server has a master system and remote management system. The master system is a Linux system. The remote management system with Integrated Lights-Out (iLO) provides remote management at the hardware-level. iLO can manage the server remotely even when the master system is restarted. The master system has two NICs bundled into an AP port for service processing. The management system uses one of the two NICs for remote management. Because services are separated by different VLANs, the VLAN used by the management system is called a management VLAN. The port of a device connected to a server with two NICs is an AP port. The packets of the management VLAN must be sent by the member port connected to the NICs of the server to ensure the communication with the remote management system. You can configure a preferred AP member port to send the packets of the management VLAN.

 For a server with two NICs bundled through LACP, if LACP is not running when the master system is restarted, LACP negotiation fails and the AP port is Down. At that time, the preferred AP member port is downgraded into a static member port and it is bound to the AP port for communication with the remote management system of the server. The preferred AP member port will be enabled with LACP again for negotiation after the Linux system is restarted and LACP runs normally.

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

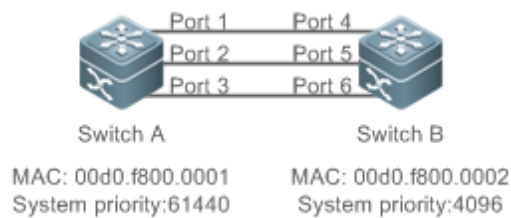
The static AP configuration is simple. Run a command to add the specified physical port to the AP port. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

- Dynamic AP (LACP)

An LACP-enabled port sends LACPDU 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
- Layer-4 source port number or Layer-4 destination port number
- Layer-4 source port number + Layer-4 destination port number
- Source IP address + Layer-4 source port number
- Source IP address + Layer-4 destination port number
- Destination IP address + Layer-4 source port number
- Destination IP address + Layer-4 destination port number
- Source IP address + Layer-4 source port number + Layer-4 destination port number
- Destination IP address + Layer-4 source port number + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number
- Source IP address + destination IP address + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number + Layer-4 destination port number
- Panel port for incoming packets
- Labels of Multiprotocol Label Switching (MPLS) packets
- Aggregation member port polling
- Enhanced mode

i 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.

i All the load balancing methods use a load algorithm (hash algorithm) to calculate the member links based on the input parameters of the methods. The input parameters include the source MAC address, destination MAC address, source MAC address + destination MAC address, source IP address, destination IP address, source IP address + destination IP addresses, source IP address + destination IP address + 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.

i 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 AP Capacity Mode	(Optional) It is used to specify the AP capacity mode.	
	aggregateport capacity mode	Configures the AP capacity mode globally.
Configuring LACP AP Ports	 (Mandatory) It is used to configure link aggregation dynamically.	
	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.	
	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.

- i** 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 <i>ap-number</i>
Parameter Description	<i>ap-number</i> : 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 <i>ap-number</i> in global configuration mode.

- i** 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.
- i** 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.
- i** 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), so the aggregation amount should match the switch limit.

↳ Configuring Static AP Member Ports

- Mandatory.
- Perform this configuration on AP-enabled devices.

Command	port-group <i>ap-number</i>
Parameter Description	<i>ap-number</i> : 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.

- i** The static AP member ports configured on the devices at both ends of a link must be consistent.

- i** 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.
- i** 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.
- i** In order to ensure the normal function, FC static AP member ports should be configured on both ends.

↘ 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 Layer-3 switches or wireless ACs that support AP functions as well as Layer-2 and Layer-3 features.

Command	no switchport
Parameter	N/A
Description	
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.

- i** 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.

↘ Creating an Ethernet AP Subinterface

- Optional.
- On a device that supports subinterface configuration, run **interface aggregateport sub-ap-number** to create a subinterface.
- Perform this configuration on AP-enabled devices that support Layer-2 and Layer-3 features, such as Layer-3 switches.

Command	interface aggregateport sub-ap-number
Parameter	<i>sub-ap-number</i> : Indicates the number of an AP subinterface.
Description	
Defaults	By default, no subinterfaces are created.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	You need to convert the master port of the AP port to a Layer-3 port before creating a subinterface.

Verification

- Run **show running** to display the configuration.
- Run **show aggregateport summary** to display the AP configuration.

Command	show aggregateport <i>aggregate-port-number</i> [load-balance summary]
Parameter Description	<i>aggregate-port-number</i> : 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.
	<pre>Ruijie# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ----- Ag18 Enabled ACCESS dst-mac Gi0/2</pre>

Configuration Example

Configuring an Ethernet Static AP Port

Scenario Figure 3-3	<p>GigabitEthernet0/1 GigabitEthernet0/3</p> <p>GigabitEthernet0/2 GigabitEthernet0/4</p> <p>Switch A Switch B</p>
Configuration Steps	<ul style="list-style-type: none"> ● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 0/3 and GigabitEthernet 0/4 ports on Switch B to static AP port 3.
Switch A	<pre>SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 0/1-2 SwitchA(config-if-range)# port-group 3</pre>
Switch B	<pre>SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 0/3-4 SwitchB(config-if-range)# port-group 3</pre>
Verification	<ul style="list-style-type: none"> ● Run show aggregateport summary to check whether AP port 3 contains member ports .
Switch A	<pre>A# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ----- Ag3 8 Enabled ACCESS Gi0/1,Gi0/2</pre>

Switch B	B# show aggregateport summary				
	AggregatePort	MaxPorts	SwitchPort	Mode	Ports
	-----	-----	-----	-----	-----
	Ag3	8	Enabled	ACCESS	Gi0/3,Gi0/4

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 <i>key-number</i> mode { active passive }
Parameter	<i>Key-number</i> : Indicates the management key of an AP port. In other words, it is the LACP AP port number.
Description	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 <i>system-priority</i>
Parameter Description	<i>system-priority</i> : 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 <i>port-priority</i>
Parameter Description	<i>port-priority</i> : Indicates the priority of an LACP member port. The value ranges from 0 to 65535.
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.

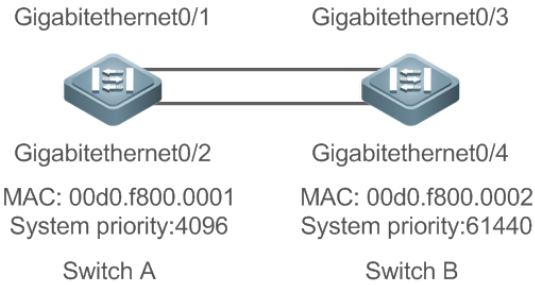
Verification

- Run **show running** to display the configuration.
- Run **show lacp summary** to display LACP link state.

Command	show lacp summary [<i>key-number</i>]
Parameter Description	<i>key-name</i> : 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 <i>key-name</i> .
	<pre> Ruijie(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. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key NumberState ----- Gi0/1SAbnd140960x30x10x3d Gi0/2SAbnd140960x30x20x3d Gi0/3SAbnd140960x30x30x3d 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 </pre>

Configuration Example

Configuring LACP

<p>Scenario Figure 3-4</p>	 <p>GigabitEthernet0/1 GigabitEthernet0/3</p> <p>GigabitEthernet0/2 GigabitEthernet0/4</p> <p>MAC: 00d0.f800.0001 MAC: 00d0.f800.0002</p> <p>System priority:4096 System priority:61440</p> <p>Switch A Switch B</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● On Switch A, set the LACP system priority to 4096. ● Enable dynamic link aggregation on the GigabitEthernet0/1 and GigabitEthernet0/2 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 GigabitEthernet0/3 and GigabitEthernet0/4 ports on Switch B and add the ports to LACP AP port 3.
<p>Switch A</p>	<pre>A# configure terminal A(config)# lacp system-priority 4096 A(config)# interface range GigabitEthernet 0/1-2 A(config-if-range)# port-group 3 mode active A(config-if-range)# end</pre>
<p>Switch B</p>	<pre>B# configure terminal B(config)# lacp system-priority 61440 B(config)# interface range GigabitEthernet 0/3-4 B(config-if-range)# port-group 3 mode active B(config-if-range)# end</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Run show lacp summary 3 to check whether LACP AP port 3 contains member ports .
<p>Switch A</p>	<pre>A#show LACP summary 3 System Id:32768, 00d0.f8fb.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State -----</pre>

	<pre> Gi0/1 SA bnd1 32768 0x3 0x10x3d Gi0/2 SA bnd1 32768 0x3 0x20x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key NumberState ----- Gi0/1 SA 32768 00d0.f800.0002 0x3 0x1 0x3d Gi0/2 SA 32768 00d0.f800.0002 0x3 0x2 0x3d </pre>
Switch B	<pre> B#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. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State ----- Gi0/3 SA bnd1 32768 0x3 0x10x3d Gi0/4 SA bnd1 32768 0x3 0x20x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key NumberState ----- Gi0/3 SA 32768 00d0.f800.0001 0x3 0x1 0x3d Gi0/4 SA 32768 00d0.f800.0001 0x3 0x2 0x3d </pre>

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 display the 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	<ul style="list-style-type: none"> ● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 0/3 and GigabitEthernet 0/4 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	<pre>A# configure terminal A(config)# interface range GigabitEthernet 0/1-2 A(config-if-range)# port-group 3 A(config-if-range)# exit A(config)# aggregateport member linktrap A(config)# interface Aggregateport 3Aggregateport3 A(config-if-AggregatePort 3)# no snmpnosnmp trap link-status</pre>
Switch B	<pre>B# configure terminal B(config)# interface range GigabitEthernet 0/3-4 B(config-if-range)# port-group 3 B(config-if-range)# exit B(config)# aggregateport member linktrap B(config)# interface Aggregateport 3Aggregateport3 B(config-if-AggregatePort 3)# no snmpnosnmp trap link-status</pre>
Verification	<ul style="list-style-type: none"> ● Run show running to check whether LinkTrap is enabled for AP port 3 and its member ports.
Switch A	<pre>A# show run include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status</pre>

	<pre>A# show run include AggregatePort aggregateport member linktrap</pre>
Switch B	<pre>B# show run include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status B# show run include AggregatePort aggregateport member linktrap</pre>

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.


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-ip dst-l4port dst-mac src-dst-ip src-dst-l4port src-dst-mac src-ip src-l4port src-mac }
Parameter Description	<p>dst-ip: Indicates that load is distributed based on the destination IP addresses of incoming packets.</p> <p>dst-l4port: Indicates that load is distributed based on Layer-4 destination port numbers.</p> <p>dst-mac: Indicates that load is distributed based on the destination MAC addresses of incoming packets.</p> <p>src-dst-ip: Indicates that load is distributed based on source and destination IP addresses of incoming packets.</p> <p>src-dst-l4port: Indicates that load is distributed based on Layer-4 source and destination port numbers.</p> <p>src-dst-mac: Indicates that load is distributed based on source and destination MAC addresses of incoming packets.</p> <p>src-ip: Indicates that load is distributed based on the source IP addresses of incoming packets.</p> <p>src-l4port: Indicates that load is distributed based on Layer-4 source port numbers.</p> <p>src-mac: Indicates that load is distributed based on the source MAC addresses of incoming packets.</p>

Defaults	Load balancing can be based on source and destination MAC addresses, source and destination IP addresses (applicable to gateways)
Command Mode	Global configuration mode
Usage Guide	<p>To restore the default settings, run no aggregateport load-balance in global configuration mode.</p> <p>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.</p> <p> 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.</p>

Configuration Example

Configuring a Load Balancing Mode

Scenario Figure 3-6	 <p>The diagram illustrates a network topology with two switches, Switch A and Switch B, connected by a single link. Switch A is on the left and has two ports labeled GigabitEthernet0/1 and GigabitEthernet0/2. Switch B is on the right and has two ports labeled GigabitEthernet0/3 and GigabitEthernet0/4. A horizontal line connects the two switches, representing the network link.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 0/3 and GigabitEthernet 0/4 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	<pre>A# configure terminal A(config)# interface range GigabitEthernet 0/1-2 A(config-if-range)# port-group 3 A(config-if-range)# exit A(config)# aggregateport load-balance src-mac</pre>
Switch B	<pre>B# configure terminal B(config)# interface range GigabitEthernet 0/3-4</pre>

	<pre>B(config-if-range)# port-group 3 B(config-if-range)# exit B(config)# aggregateport load-balance dst-mac</pre>
Verification	<ul style="list-style-type: none"> Run show aggregateport load-balance to check the load balancing algorithm configuration.
Switch A	<pre>A# show aggregatePort load-balance Load-balance : Source MAC</pre>
Switch B	<pre>B# show aggregatePort load-balance Load-balance : Destination MAC</pre>

↘ Configuring Hash Load Balancing Control

Common Errors

3.4.5 Configuring an AP Capacity Mode

Configuration Effect

- Change the maximum number of configurable AP ports and the maximum number of member ports in each AP port.

Notes

- The system has a default AP capacity mode. You can run **show aggregateport capacity** to display the current capacity mode.
- If the current configuration (maximum number of AP ports or the number of member ports in each AP port) exceeds the capacity to be configured, the capacity mode configuration will fail.

Configuration Steps

↘ Configuring an AP Capacity Mode

- (Optional) Perform this configuration to change the AP capacity.
- Perform this configuration on devices that support AP capacity change, such as core switches.

Command	aggregateport capacity mode <i>capacity-mode</i>
Parameter	<i>capacity-mode</i> : Indicates a capacity mode.
Description	
Defaults	By default, AP capacity modes vary with devices. For example, 8 x 8 indicates that the device has a maximum of 8 AP ports and 8 member ports in each AP port.
Command Mode	Global configuration mode
Usage Guide	The system provides several capacity modes for devices that support capacity mode configuration. To

restore the default settings, run **no aggregateport capacity mode** in global configuration mode.

Verification

- Run **show running** to display the configuration.
- Run **show aggregateport capacity** to display the current AP capacity mode and AP capacity usage.

Command	show aggregateport capacity
Parameter Description	N/A
Command Mode	Any mode
Usage Guide	N/A
	<pre>Ruijie# show aggregateport capacity AggregatePort Capacity Information: Configuration Capacity Mode: 8*8. Effective Capacity Mode : 8*8. Available Capacity : 8*8. Total Number: 8, Used: 1, Available: 7.</pre>

Configuration Example

Configuring an AP Capacity Mode

Scenario Figure 3-7	<p>The diagram illustrates a network topology with two switches, Switch A and Switch B, connected by a single link. Switch A is on the left and has two ports labeled GigabitEthernet0/1 and GigabitEthernet0/2. Switch B is on the right and has two ports labeled GigabitEthernet0/3 and GigabitEthernet0/4. A horizontal line connects the two switches, representing the network link.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 0/3 and GigabitEthernet 0/4 ports on Switch B to static AP port 3. ● On Switch A, configure the 8*8 AP capacity mode. ● On Switch B, configure the 8*8 AP capacity mode.
Switch A	<pre>A# configure terminal A(config)# interface range GigabitEthernet 0/1-2 A(config-if-range)# port-group 3 A(config-if-range)# exit A(config)# aggregateport capacity mode 8*8</pre>


Switch B	<pre>B# configure terminal B(config)# interface range GigabitEthernet 0/3-4 B(config-if-range)# port-group 3 B(config-if-range)# exit B(config)# aggregateport capacity mode 8*8</pre>
Verification	<ul style="list-style-type: none"> Run show aggregateport capacity to check the AP capacity mode configuration.
Switch A	<pre>A# show aggregatePort capacity AggregatePort Capacity Information: Configuration Capacity Mode: 8*8. Effective Capacity Mode : 8*8 Available Capacity Mode : 8*8 Total Number : 8, Used: 1, Available: 7.</pre>
Switch B	<pre>B# show aggregatePort capacity AggregatePort Capacity Information: Configuration Capacity Mode: 8*8 Effective Capacity Mode : 8*8 Available Capacity Mode : 8*8 Total Number : 8, Used: 1, Available: 7</pre>

3.5 Monitoring

Displaying

Description	Command
Displays the LACP aggregation state. You can display the information on a specified LACP AP port by specifying <i>key-number</i> .	show lacp summary [<i>key-number</i>]
Displays the summary or load balancing algorithm of an AP port.	show aggregateport [<i>ap-number</i>] { 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 { all database event ha packet realtime stm timer }

4 Configuring VLAN

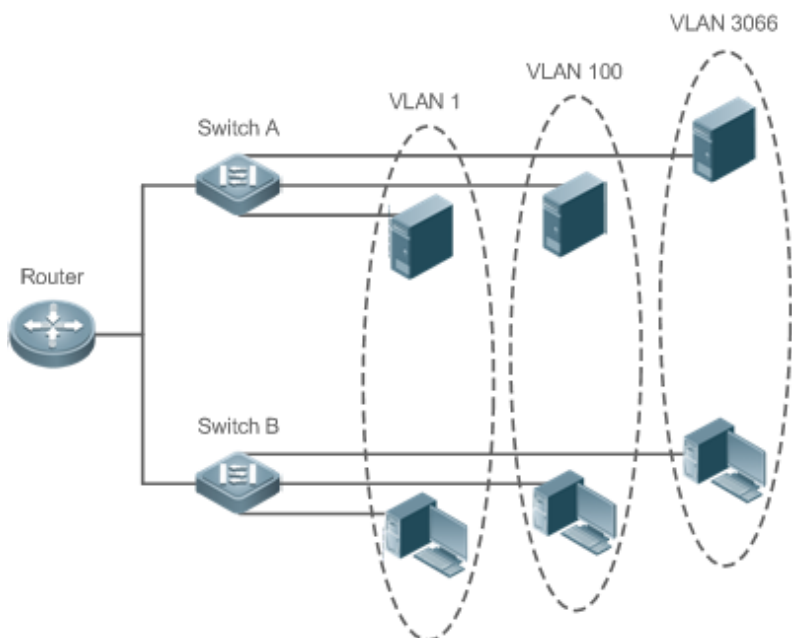
4.1 Overview

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

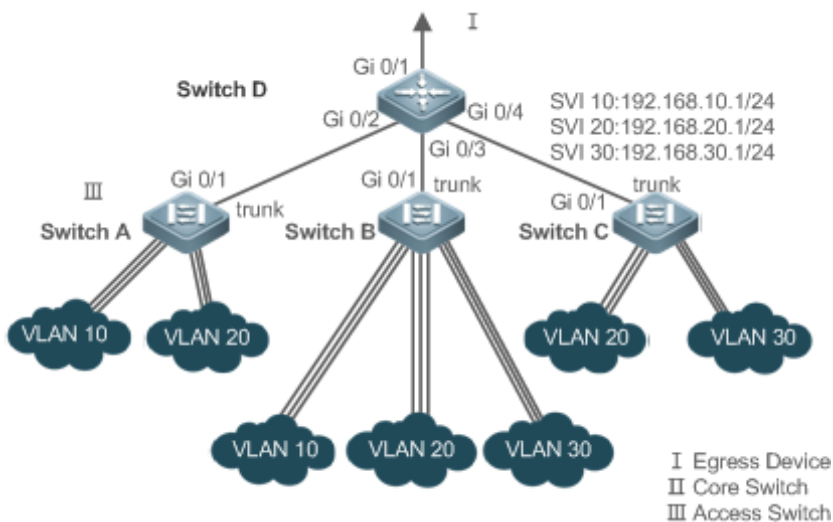
Application	Description
Isolating VLANs at Layer 2 and Interconnecting VLANs at Layer 3	An intranet is divided into multiple VLANs, realizing Layer-2 isolation and Layer-3 interconnection with each other through IP forwarding by core switches.

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	<p>Switch A, Switch B and Switch C are access switches.</p> <p>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;</p> <p>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.</p> <p>Create VLANs respectively on the three access switches, assign Access ports for the VLANs, and specify Trunk ports of the core switch.</p>
----------------	---

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.

- i** The VLANs supported by Ruijie 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.
- i** The configurable VLAN IDs are from 1 to 4094.
- i** 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.
	 (Optional) It is used to restore the port mode.
	no switchport mode Restores the port mode to 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 configure Uplink ports to transmit flows from multiple VLANs.
	switchport trunk allowed vlan Configures allowed-VLANs for a Uplink port.
	switchport trunk native vlan Specifies a native VLAN for a Uplink port.
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.
	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 VLAN2 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	<code>vlan { <i>vlan-id</i> range <i>vlan-range</i> }</code>
Parameter	<i>vlan-id</i> : indicates VLAN ID ranging from 1 to 4094.
Description	range <i>vlan-range</i> : indicates VLAN ID range.
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 <i>vlan-id</i> 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	<code>name <i>vlan-name</i></code>
Parameter	<i>vlan-name</i> : indicates a VLAN name.
Description	
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 <i>vlan-id</i>
Parameter Description	<i>vlan-id</i> : 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 { <i>interface-id</i> range <i>interface-range</i> }
Parameter	<i>interface-id</i> : indicates a single port.
Description	<i>interface-id</i> : 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 <i>vlan-id</i> .

i 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 [<i>id</i> <i>vlan-id</i>]						
Parameter Description	<i>vlan-id</i> : indicates a VLAN ID.						
Command Mode	Any mode						
Usage Guide	N/A						
Command Display	<pre>Ruijie(config-vlan)# show vlan id 20</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>20 VLAN0020</td> <td>STATIC</td> <td>Gi0/1</td> </tr> </tbody> </table>	VLAN Name	Status	Ports	20 VLAN0020	STATIC	Gi0/1
VLAN Name	Status	Ports					
20 VLAN0020	STATIC	Gi0/1					

Configuration Example

➤ Configuring Basic VLAN and Access Port

Configuration Steps	<ul style="list-style-type: none"> ● Create a VLAN and rename it. ● Add an Access port to the VLAN. There are two approaches. <p>One is:</p> <pre>Ruijie# configure terminal Ruijie(config)# vlan 888 Ruijie(config-vlan)# name test888 Ruijie# configure terminal Ruijie(config)# interface GigabitEthernet 0/3</pre>
----------------------------	--

	<pre>Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport access vlan 20</pre> <p>The other approach is adding an Access port (GigabitEthernet 0/3) to VLAN20:</p> <pre>Ruijie# configure terminal Ruijie(config)# vlan 20 Ruijie(config-vlan)# add interface GigabitEthernet0/3</pre>																		
Verification	Check whether the configuration is correct.																		
	<pre>Ruijie(config-vlan)# show vlan</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>1 VLAN0001</td> <td>STATIC</td> <td></td> </tr> <tr> <td>20 VLAN0020</td> <td>STATIC</td> <td>Gi0/3</td> </tr> <tr> <td>888 test888</td> <td>STATIC</td> <td></td> </tr> </tbody> </table> <pre>Ruijie(config-vlan)#</pre> <pre>Ruijie#show interfaceGigabitEthernet0/3 switchport</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>Switchport Mode</th> <th>Access Native Protected VLAN lists</th> </tr> </thead> <tbody> <tr> <td>GigabitEthernet 0/3</td> <td>enabled ACCESS</td> <td>20 1 Disabled ALL</td> </tr> </tbody> </table>	VLAN Name	Status	Ports	1 VLAN0001	STATIC		20 VLAN0020	STATIC	Gi0/3	888 test888	STATIC		Interface	Switchport Mode	Access Native Protected VLAN lists	GigabitEthernet 0/3	enabled ACCESS	20 1 Disabled ALL
VLAN Name	Status	Ports																	
1 VLAN0001	STATIC																		
20 VLAN0020	STATIC	Gi0/3																	
888 test888	STATIC																		
Interface	Switchport Mode	Access Native Protected VLAN lists																	
GigabitEthernet 0/3	enabled ACCESS	20 1 Disabled ALL																	

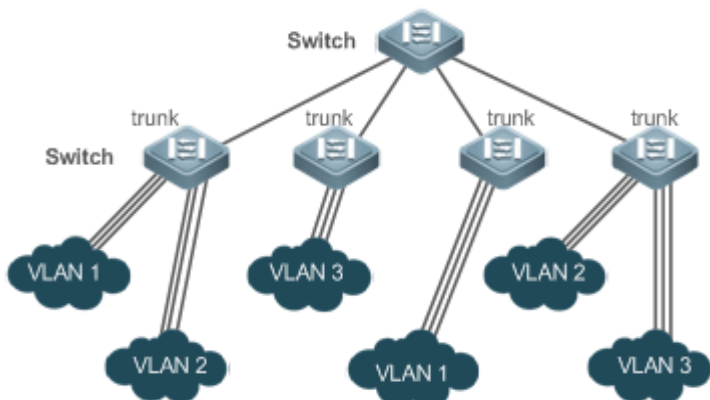
4.4.2 Configuring a Trunk Port

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 Ruijie 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	N/A
Description	
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 <i>vlan-list</i> 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 <i>vlan-list</i> : indicates adding a specific VLAN to the list of allowed-VLANs; remove <i>vlan-list</i> : indicates removing a specific VLAN from the list of allowed-VLANs; except <i>vlan-list</i> : indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs. only <i>vlan-list</i> : 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 <i>vlan-id</i>
Parameter Description	<i>vlan-id</i> : 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.

i 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 interfaces witch port** to check whether the configuration takes effect.

Command	show vlan [id <i>vlan-id</i>]								
Parameter Description	<i>vlan-id</i> : indicates a VLAN ID.								
Command Mode	Any mode								
Usage Guide	N/A								
Command Display	<pre>Ruijie(config-vlan)# show vlan id 20</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>20 VLAN0020</td> <td>STATIC</td> <td>Gi0/1</td> </tr> </tbody> </table>			VLAN Name	Status	Ports	20 VLAN0020	STATIC	Gi0/1
VLAN Name	Status	Ports							
20 VLAN0020	STATIC	Gi0/1							

Configuration Example

Configuring Basic VLAN to Realize Layer-2 Isolation and Layer-3 Interconnection

<p>Scenario Figure 4-4</p>	
<p>Configuration Steps</p>	<p>Networking Requirements:</p> <p>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.</p> <p>Key Points:</p> <p>The following example describes the configuration steps on a core switch and an access switch.</p> <ul style="list-style-type: none"> ● 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.

<p>D</p>	<pre>D#configure terminal D(config)# vlan10 D(config-vlan)# vlan20 D(config-vlan)# vlan30 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 0/2)# switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan add 10,20,30 D(config-if-GigabitEthernet 0/2)# interface GigabitEthernet0/4 D(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan add 20,30 D(config-if-GigabitEthernet 0/2)# exit 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</pre>
<p>A</p>	<pre>A# configure terminal A(config)# vlan10 A(config-vlan)# vlan20 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</pre>
<p>Verification</p>	<p>Display the VLAN configuration on the core switch.</p> <ul style="list-style-type: none"> ● 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.
<p>D</p>	<pre>D#show vlan VLANName Status Ports</pre>

```

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 GigabitEthernet0/3 switchport
Interface          Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/3      enabled TRUNK 1      1      Disabled 10,20,30
D#show interface GigabitEthernet0/4switchport
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	Interface configuration mode

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 <i>vlan-list</i> remove <i>vlan-list</i> except <i>vlan-list</i> only <i>vlan-list</i> }
Parameter Description	The parameter <i>vlan-list</i> 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 <i>vlan-list</i> : indicates adding a specific VLAN to the list of allowed-VLANs; remove <i>vlan-list</i> : indicates removing a specific VLAN from the list of allowed-VLANs; except <i>vlan-list</i> : indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs; and only <i>vlan-list</i> : 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 <i>vlan-id</i>
Parameter Description	<i>vlan-id</i> : 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 <i>vlan-id</i>]
Parameter	<i>vlan-id</i> : indicates a VLAN ID.

Description							
Command Mode	Any mode						
Usage Guide	N/A						
Command Display	<pre>Ruijie(config-vlan)# show vlan id 20</pre> <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>Status</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>20 VLAN0020</td> <td>STATIC</td> <td>Gi0/1</td> </tr> </tbody> </table>	VLAN Name	Status	Ports	20 VLAN0020	STATIC	Gi0/1
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.												
	<pre>Ruijie# configure terminal Ruijie(config)# interface gi 0/1 Ruijie(config-if-GigabitEthernet 0/1)# switchport mode uplink Ruijie(config-if-GigabitEthernet 0/1)# end</pre>												
Verification	Check whether the configuration is correct.												
	<pre>Ruijie# show interfaces GigabitEthernet 0/1switchport</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>Switchport Mode</th> <th>Access</th> <th>Native</th> <th>Protected</th> <th>VLAN lists</th> </tr> </thead> <tbody> <tr> <td>GigabitEthernet 0/1</td> <td>enabled UPLINK</td> <td>1</td> <td>1</td> <td>disabled</td> <td>ALL</td> </tr> </tbody> </table>	Interface	Switchport Mode	Access	Native	Protected	VLAN lists	GigabitEthernet 0/1	enabled UPLINK	1	1	disabled	ALL
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	N/A

Description	
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] tagged [add] untagged only tagged remove } <i>vlan-list</i>
Parameter Description	<i>vlan-list</i> : Specifies the VLAN; add : Adds the port to the VLAN; only tagged <i>vlist</i> : Adds the port to the VLAN and removes the port from the VLANs not on the VLAN list; [add] tagged <i>vlist</i> : Adds the port to the VLAN and the VLAN packets going out on the port are tagged with VLAN ID; [add] untagged <i>vlist</i> : Adds the port to the VLAN and the VLAN packets going out on the port are not tagged with VLAN ID; remove <i>vlist</i> : Removes the port from the VLAN.
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 <i>vlan_id</i>
Parameter Description	<i>vlan-id</i> : indicates a VLAN ID.
Defaults	The default native VLAN is VLAN 1.
Command Mode	Interface configuration 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 a 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 <i>vlan-id</i>]		
Parameter Description	<i>vlan-id</i> : indicates a VLAN ID.		
Command Mode	Any mode		
Usage Guide	N/A		
Command Display	<pre>Ruijie(config-vlan)# show vlan id 20 VLAN Name Status Ports ----- 20 VLAN0020 STATIC Gi0/1</pre>		

Configuration

Example

Configuring a Hybrid Port

Configuration Steps	The following is an example of configuring Gi0/1 as a Hybrid port.
	<pre>Ruijie# configure terminal Ruijie(config)# interface gigabitEthernet0/1 Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3 Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20-30 Ruijie(config-if-GigabitEthernet 0/1)# end</pre>
Verification	Check whether the configuration is correct.
	<pre>Ruijie(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</pre>

4.5 Monitoring

Displaying

Description	Command
Displays VLAN configuration.	show vlan [id <i>vlan-id</i>]
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 MAC VLAN

5.1 Overview

The MAC VLAN function refers to assigning VLANs based on MAC addresses, which is a new method of VLAN assignment. This function is often used with 802.1Xdynamic VLAN assignment to implement secure and flexible access of 802.1Xterminals. After an 802.1Xuser passes authentication, the access switch automatically generates a MAC VLAN entry based on the VLAN and user MAC address pushed by the authentication server. A network administrator can also configure the association between a MAC address and a VLAN on the switch in advance.

Protocols

- IEEE 802.1Q: Virtual Bridged Local Area Networks and Standards

5.2 Applications

Application	Description
Configuring MAC VLAN	Configures the MAC VLAN function to assign VLANs based on users' MAC addresses. When the physical location of a user changes, i.e. switching from one switch to another, it is unnecessary to re-configure the VLAN of the port used by the user.

5.2.1 Configuring MAC VLAN

Scenario

With popularization of mobile office, terminal devices usually do not use fixed ports for network access. A terminal device may use port A to access the network this time, but use port B to access the network next time. If the VLAN configurations of ports A and B are different, the terminal device will be assigned to a different VLAN in the second access, and fail to use the resources of the previous VLAN. If the VLAN configurations of ports A and B are the same, security issues may be introduced when port B is assigned to other terminal devices. How to allow hosts of different VLANs to access the network on the same port? The MAC VLAN function is hereby introduced.

The biggest advantage of MAC VLAN lies in that when the physical location of a user changes, i.e. switching from one switch to another, it is unnecessary to re-configure the VLAN of the port used by the user. Therefore, MAC address-based VLAN assignment can be regarded as user-based.

Deployment

- Configure or push MAC VLAN entries on a layer-2 switch or wireless device to assign VLANs based on users' MAC addresses.

5.3 Overview

Feature

Feature	Description
Configuring MAC VLAN	Configures the MAC VLAN function to assign VLANs based on users' MAC addresses.

5.3.1 Configuring MAC VLAN







Working Principle

When a switch receives a packet, the switch compare the source MAC address of the packet with the MAC address specified in a MAC VLAN entry. If they match, the switch forwards the packet to the VLAN specified in the MAC VLAN entry. If they don't match, the VLAN to which the data stream belongs is still determined by the VLAN assignment rule of the port.



To ensure that a PC is assigned to a specified VLAN no matter which switch it is connected to, you can perform configuration by using the following approaches:

- Static configuration by using commands. You can configure the association between a MAC address and a VLAN on a local switch by using commands.
- Automatic configuration by using an authentication server (802.1Xdynamic VLAN assignment). After a user passes authentication, a switch dynamically creates an association between the MAC address and a VLAN based on the information provided by the authentication server. When the user goes offline, the switch automatically deletes the association. This approach requires that the MAC-VLAN association be configured on the authentication server. For details about 802.1Xdynamic VLAN assignment, refer to the Configuring 802.1X.

MAC VLAN entries support both of the two approaches, that is, the entries can be configured on both a local switch and an authentication server. The configurations can take effect only if they are consistent. If the configurations are different, the configuration performed earlier takes effect.

-  The MAC VLAN function can be configured on hybrid ports only.
-  MAC VLAN entries are effective only for untagged packets, but not effective for tagged packets.
-  For MAC VLAN entries statically configured or dynamically generated, the specified VLANs must exist.
-  VLANs specified in MAC VLAN entries cannot be Super VLANs (but can be Sub VLANs), Remote VLANs, or Primary VLANs (but can be Secondary VLANs).
-  MAC addresses specified in MAC VLAN entries must be unicast addresses.
-  MAC VLANs are effective for all hybrid ports that are enabled with the MAC VLAN function.

5.4 Configuration

Configuration	Description and Command
Enabling MAC VLAN on a Port	 (Mandatory) It is used to enable the MAC VLAN function on a port.
	mac-vlan enable Enables MAC VLAN on a port.
Adding a Static MAC VLAN Entry Globally	 (Optional) It is used to bind MAC addresses with VLANs.
	mac-vlan mac-address Configures a static MAC VLAN entry.

5.4.1 Enabling MAC VLAN on a Port

Configuration Effect

Enable the MAC VLAN function on a port so that MAC VLAN entries can take effect on the port.

Notes

N/A

Configuration Steps

▾ Enabling MAC VLAN on a Port

- Mandatory.
- By default, the MAC VLAN function is disabled on ports and all MAC VLAN entries are ineffective on the ports.
- Enable MAC VLAN on a switch.

Command	mac-vlan enable
Parameter Description	N/A
Defaults	The MAC VLAN function is disabled on a port.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Run the **show mac-vlan interface** command to display information about the ports enabled with the MAC VLAN function.

Command	show mac-vlan interface
Parameter Description	N/A
Command Mode	Privileged configuration mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
Command Display	<pre>Ruijie# show mac-vlan interface MAC VLAN is enabled on following interface: ----- GigabitEthernet 0/1</pre>

Configuration

Example

▾ Enabling MAC VLAN on a Port

Configuration Steps	<ul style="list-style-type: none"> ● Enable the MAC VLAN function on the Fast Ethernet 0/10 port.
----------------------------	--

	<pre>Ruijie# configure terminal Ruijie(config)# interface gigabitethernet0/10 Ruijie(config-if-GigabitEthernet 0/10)# mac-vlan enable</pre>
Verification	<ul style="list-style-type: none"> ● Check the information about the port enabled with the MAC VLAN function.
	<pre>Ruijie# show mac-vlan interface MAC VLAN is enabled on following interface: ----- GigabitEthernet 0/10</pre>

Common Errors

When the MAC VLAN function is enabled on a port, the port is not configured as a layer-2 port (such as switch port or AP port) in advance.

5.4.2 Adding a Static MAC VLAN Entry Globally

Configuration Effect

- Configure a static MAC VLAN entry to bind a MAC addresses with a VLAN.

Notes

N/A

Configuration Steps

▾ Adding a Static MAC VLAN Entry

- Optional.
- To bind a MAC addresses with a VLAN, you should perform this configuration.
- Add a static MAC VLAN entry on a switch.

Command	mac-vlan mac-address <i>mac-address</i> [mask <i>mac-mask</i>] vlan <i>vlan-id</i>
Parameter Description	mac-address <i>mac-address</i> : Indicates a MAC address. mask <i>mac-mask</i> : Indicates a mask. vlan <i>vlan-id</i> : Indicates the associated VLAN.
Defaults	No static MAC VLAN entry is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

i If an untagged packet is matched with a MAC VLAN entry, the packet is modified to the VLAN specified by the MAC VLAN entry once arriving at the switch since the MAC VLAN entry has the highest priority. Subsequent functions and protocols are implemented based on the modified VLAN. Possible influences are as follows:

- i** If an 802.1X user fails to be authenticated, the hybrid port jumps to VLAN 100 specified by the FAIL VLAN function; however, the MAC VLAN entry statically configured redirects all packets of this user to VLAN 200. Consequently, the user cannot implement normal communication in FAIL VLAN 100.
- i** After an untagged packet is matched with a MAC VLAN entry, the VLAN that triggers MAC address learning is the VLAN redirected based on the MAC VLAN entry.
- i** For a port that is enabled with the MAC VLAN function, if received packets are matched with both MAC VLAN entries with full F masks and those without full F masks, the packets are processed based on the MAC VLAN entries without full F masks.
- i** If an untagged packet is matched with both a MAC VLAN entry and a PROTOCOL VLAN entry, the VLAN carried in the packet should be the MAC VLAN.
- i** The MAC VLAN function is applied only to untagged packets, but not applied to PRIORITY packets (packets whose VLAN tag is 0 and carrying COS PRIORITY information) and the processing actions are uncertain.

↘ Deleting All Static MAC VLAN Entries

- Optional.
- To delete all static MAC VLAN entries, you should perform this configuration.
- Perform this configuration on a switch.

Command	no mac-vlan all
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Deleting the Static MAC VLAN Entry of a Specified MAC Address

- Optional.
- To delete the MAC VLAN entry of a specified MAC address, you should perform this configuration.
- Perform this configuration on a switch.

Command	no mac-vlan mac-address <i>mac-address</i> [mask <i>mac-mask</i>]
Parameter Description	mac-address <i>mac-address</i> : Indicates a MAC address. mask <i>mac-mask</i> : Indicates a mask.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Deleting the Static MAC VLAN Entry of a Specified VLAN

- Optional.
- To delete the MAC VLAN entry of a specified VLAN, you should perform this configuration.
- Perform this configuration on a switch.

Command	no mac-vlan vlan <i>vlan-id</i>
Parameter Description	vlan <i>vlan-id</i> : Indicates a VLAN.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show mac-vlan static** command to check whether all static MAC VLAN entries are correct.
- Run the **show mac-vlan vlan** *vlan-id* command to check whether the MAC VLAN entry of a specified VLAN is correct.
- Run the **show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] command to display the MAC VLAN entry of a specified MAC address.

Command	show mac-vlan static show mac-vlan vlan <i>vlan-id</i> show mac-vlan mac-address <i>mac-address</i> [mask <i>mac-mask</i>]
Parameter Description	vlan <i>vlan-id</i> : Indicates a specified VLAN. mac-address <i>mac-address</i> : Indicates a specified MAC address. mask <i>mac-mask</i> : Indicates a specified mask.
Command Mode	Privileged configuration mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
Command Display	<pre>Ruijie# show mac-vlan all The following MAC VLAN address exist: S: Static D: Dynamic MAC ADDR MASK VLAN ID Prio STATE ----- 0000.0000.0001 ffff.ffff.ffff 2 0 D 0000.0000.0002 ffff.ffff.ffff 3 0 S 0000.0000.0003 ffff.ffff.ffff 3 0 S&D Total MAC VLAN address count: 3</pre>

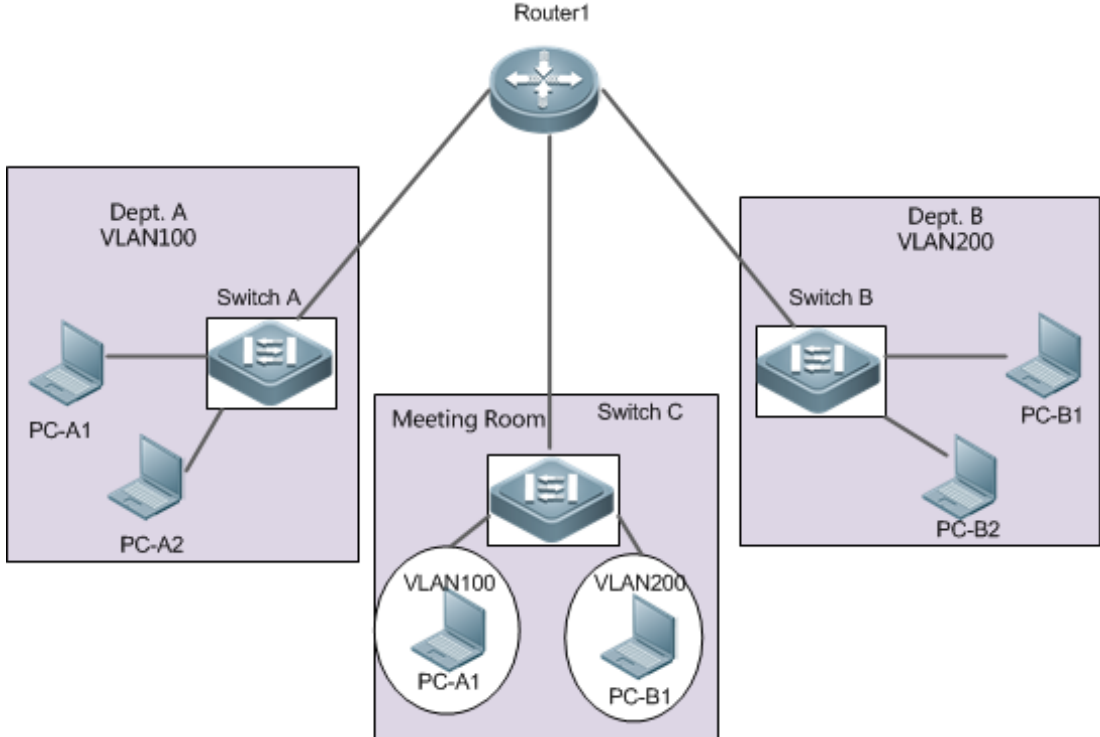
Configuration

Example

Adding a Static MAC VLAN Entry Globally

As shown in Figure 5-1, PC-A1 and PC-A2 belong to department A and are assigned to VLAN 100. PC-B1 and PC-B2 belong to department B and are assigned to VLAN 200. Due to employee mobility, the company provides a temporary office at the meeting room but requires that accessed employees be assigned to the VLANs of their own departments. For example, PC-A1 must be assigned to VLAN 100 and PC-B1 must be assigned to VLAN 200 after access.

Since the access ports for PCs at the meeting room are not fixed, the MAC VLAN function can be used to associate the PC MAC addresses with the VLANs of their departments. No matter which ports the employees use for access, the MAC VLAN function automatically assigns the VLANs of their departments.

<p>Scenario Figure 5-1</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure the port connecting Switch C and Router 1 as a Trunk port. ● Configure all ports connecting PCs on Switch C as hybrid ports, enable the MAC VLAN function and modify the default untagged VLAN list. ● Configure MAC VLAN entries on Switch C.
<p>Switch C</p>	<pre>SwitchC# configure terminal SwitchC(config)# interface interface_name SwitchC(config-if)# switchport mode trunk SwitchC(config-if)# exit SwitchC(config)# interface interface_name SwitchC(config-if)# switchport mode hybrid SwitchC(config-if)# switchport hybrid allowed vlan add untagged 100,200 SwitchC(config-if)# mac-vlan enable SwitchC(config-if)# exit SwitchC(config)# mac-vlan mac-address PC-A1-mac vlan 100 SwitchC(config)# mac-vlan mac-address PC-B1-mac vlan 200</pre>
<p>Verification</p>	<p>Check the configured static MAC VLAN entries on Switch C.</p>
<p>Switch C</p>	<pre>SwitchC# show mac-vlan static</pre>

The following MAC VLAN address exist:				
S: Static D: Dynamic				
MAC ADDR	MASK	VLAN ID	PRIO	STATE

PC-A1-mac	ffff.ffff.ffff	100	0	S
PC-B1-mac	ffff.ffff.ffff	200	0	S
Total MAC VLAN address count: 2				

5.5 Monitoring

Displaying

Description	Command
Displays all the MAC VLAN entries, including static and dynamic.	show mac-vlan all
Displays the dynamic MAC VLAN entries.	show mac-vlan dynamic
Displays the static MAC VLAN entries.	show mac-vlan static
Displays the MAC VLAN entries of a specified VLAN.	show mac-vlan vlan <i>vlan-id</i>
Displays the MAC VLAN entries of a specified MAC address.	show mac-vlan mac-address <i>mac-address</i> [mask <i>mac-mask</i>]

Debugging



System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the MAC VLAN function.	debug bridge mvlan

6 Configuring Protocol VLAN

6.1 Overview

The protocol VLAN technology is a VLAN distribution technology based on the packet protocol type. It can distribute packets of a certain protocol type with a null VLAN ID to the same VLAN. That is, the switch, based on the protocol type and encapsulation format of packets received by ports, matches the received untagged packets with protocol profiles. If the matching is successful, the switch automatically distributes the packets to a relevant VLAN for transmission. There are two types of protocol VLANs: IP address-based protocol VLAN and protocol VLAN based on the packet type and Ethernet type on ports. The protocol VLAN based on the packet type and Ethernet type on ports is called protocol VLAN for short and the IP address-based protocol VLAN is called subnet VLAN for short.

i The protocol VLAN is applicable only to Trunk ports and Hybrid ports.

Protocols and Standards

IEEE standard 802.1Q

6.2 Applications

Application	Description
Configuration and Application of Protocol VLAN	Implements Layer-2 communication isolation of user hosts that use different protocol packets for communication to reduce the network traffic.
Configuration and Application of Subnet VLAN	Specifies the VLAN range based on the IP network segment to which user packets belong.

6.2.1 Configuration and Application of Protocol VLAN

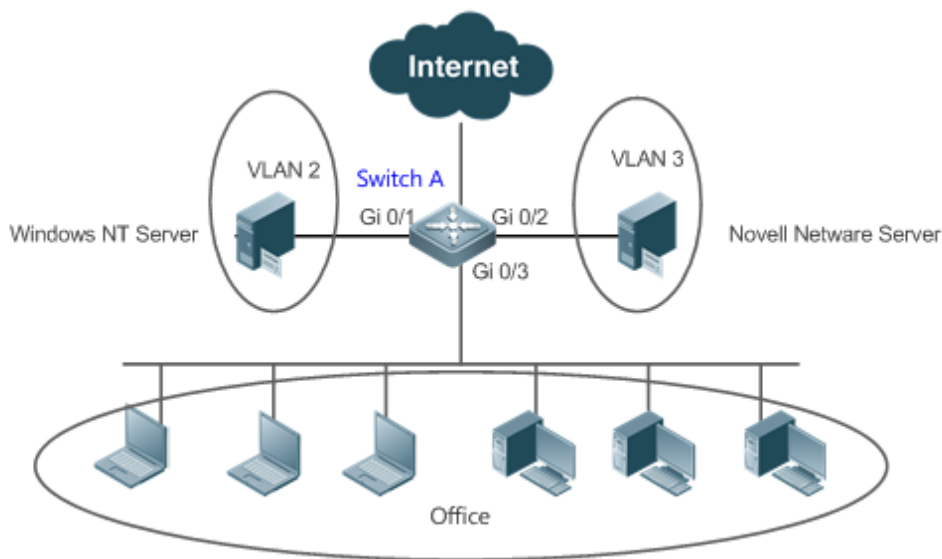
Scenario

As shown in the following figure, the network architecture is composed of the interconnected Windows NT server and Novell Netware server and the office area is connected to the Layer-3 device Switch A through a hub. There are different PCs in the office area. Some PCs use the Windows NT operating system (OS) and support the IP protocol, and some PCs use the Novell Netware OS and support the IPX protocol. PCs in the office area communicate with the external network and servers through the uplink port Gi 0/3.

The main requirements are as follows:

- The Layer-2 communication of PCs using the Windows NT OS is isolated from that of PCs using the Novell Netware OS, so as to reduce the network traffic.

Figure 6-1



Remarks	Switch A is a switch and Port Gi 0/3 is a Hybrid port. Port Gi 0/1 is an Access port and belongs to VLAN 2. Port Gi 0/2 is also an Access port and belongs to VLAN 3.
----------------	---

Deployment

- Configure profiles of the packet type and Ethernet type (in this example, configure Profile 1 for IP protocol packets and configure Profile 2 for IPX protocol packets).
- Apply the profiles to the uplink port (Port Gi 0/3 in this example) and associate them with VLANs (in this example, associate Profile 1 with VLAN 2 and associate Profile 2 with VLAN 3).

The configured protocol VLANs take effect only on the Trunk ports and Hybrid ports.

6.2.2 Configuration and Application of Subnet VLAN

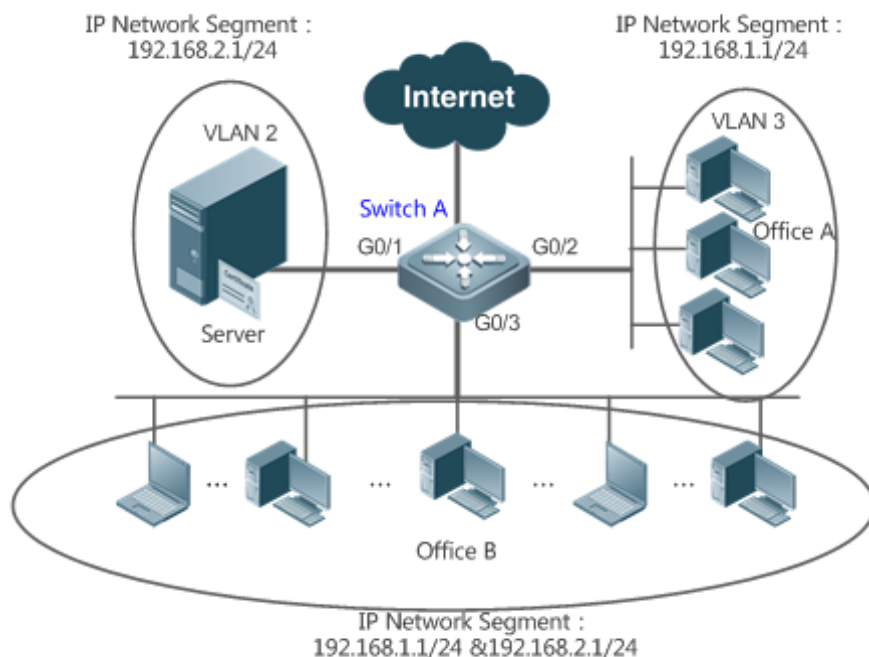
Scenario

As shown in the following figure, PCs in Office A and Office B are connected to the Layer-3 device Switch A through hubs. In Office A, the PCs belong to a fixed network segment and they are distributed to the same VLAN by port. In Office B, the PCs belong to two network segments, but they cannot be distributed to VLANs by fixed port.

The main requirements are as follows:

For PCs in Office B, Switch A can determine the VLAN range of the PCs based on the IP network segment to which their packets belong.

Figure 6-2



Remarks	Switch A is a switch. Port G0/1 is an Access port and belongs to VLAN 2. Port G0/2 is also an Access port and belongs to VLAN 3. Port G0/3 is a Hybrid port.
----------------	--

Deployment

- Globally configure subnet VLANs (in this example, allocate the IP network segment 192.168.1.1/24 to VLAN 3 and the IP network segment 192.168.2.1/24 to VLAN 2) and enable the subnet VLAN function on the uplink port (Port Gi 0/3 in this example).

! The configured subnet VLANs take effect only on the Trunk ports and Hybrid ports.

6.3 Features

Basic Concepts

Protocol VLAN

The protocol VLAN technology is a VLAN distribution technology based on the packet protocol type. It can distribute packets of a certain protocol type with a null VLAN ID to the same VLAN.

VLANs need to be specified for packets received by device ports so that a packet belongs to a unique VLAN. There are three possible cases:

- If a packet contains a null VLAN ID (untagged or priority packet) and the device supports only port-based VLAN distribution, the VLAN ID in the tag added to the packet is the PVID of the input port.
- If a packet contains a null VLAN ID (untagged or priority packet) and the device supports VLAN distribution based on the packet protocol type, the VLAN ID in the tag added to the packet is selected from the VLAN IDs mapped to

the protocol suite configuration of the input port. If the protocol type of the packet does not match all protocol suite configuration of the input port, a VLAN ID is allocated according to the port-based VLAN distribution.

- If a packet is a tagged packet, the VLAN to which the packet belongs is determined by the VLAN ID in the tag.

Subnet VLANs can be configured only globally that is, only the protocol VLAN function can be enabled or disabled on ports. The matching configuration is globally performed for the protocol VLAN, the matching configuration is selected on ports and the VLAN IDs are specified for packets that are matched successfully.

- If an input packet contains a null VLAN ID and the IP address of the input packet matches an IP address, the packet is distributed to the subnet VLAN.
- If an input packet contains a null VLAN ID and the packet type and Ethernet type of the input packet match the packet type and Ethernet type of an input port, the packet is allocated to the protocol VLAN.

📌 **Protocol VLAN Priority**

The priority of a subnet VLAN is higher than that of a protocol VLAN. That is, if a subnet VLAN and protocol VLAN are configured at the same time and an input packet conforms to both the subnet VLAN and protocol VLAN, the subnet VLAN prevails.

Overview


Feature	Description
Automatic VLAN Distribution Based on Packet Type	The service types supported on a network are bound with VLANs or packets from a specified IP network segment are transmitted in a specified VLAN to facilitate management and maintenance.


6.3.1 Automatic VLAN Distribution Based on Packet Type

Working Principle

Set rules on the hardware and enable the rules on ports. The rules take effect only after they are enabled on ports. The rules include the packet type and IP address of packets. When a port receives untagged data packets that meet the rules, the port automatically distributes them to the VLAN specified in the rules for transmission. When the rules are disabled on ports, untagged data packets are distributed to the Native VLAN according to the port configuration.

6.4 Configuration

Configuration	Description and Command
Configuring the Protocol VLAN Function	 (Mandatory) It is used to enable the VLAN distribution function based on the packet type and Ethernet type of the protocol VLAN.
	<code>protocol-vlan profile num frame-type { EtherII ether-type type SNAP ether-type type LLC dsap value ssap value }</code> Configures the profile of the packet type and Ethernet type.
	<code>protocol-vlan profile num vlan vlan-id</code> (Interface configuration mode) Applies the protocol VLAN on a port.

Configuration	Description and Command	
Configuring the Subnet VLAN Function	 (Mandatory) It is used to enable IP address-based VLAN distribution function of the protocol VLAN.	
	protocol-vlan ipv4 <i>ip-addr mask mask-addr</i> vlan <i>vlan-id</i>	Configures an IP address, subnet mask, and VLAN distribution.
	protocol-vlan ipv4	(Interface configuration mode) Enables the subnet VLAN on a port.

6.4.1 Configuring the Protocol VLAN Function

Configuration Effect

Bind service types supported in a network with VLANs to facilitate management and maintenance.

Notes

- It is recommended that the protocol VLAN be configured after VLANs, and the Trunk, Hybrid, Access, and AP attributes of ports are configured.
- If protocol VLAN is configured on a Trunk port or Hybrid port, all VLANs relevant to the protocol VLAN need to be contained in the permitted VLAN list of the Trunk port or Hybrid port.

Configuration Steps

▾ Configuring the Protocol VLAN Globally

- Mandatory.
- The protocol VLAN can be applied on an interface only in global configuration mode.

Command	protocol-vlan profile <i>num</i> frame-type { EtherII ether-type <i>type</i> SNAP ether-type <i>type</i> LLC dsap <i>value</i> ssap <i>value</i> }
Parameter Description	profile <i>num</i> : Indicates the profile index. EtherII ether-type <i>type</i> : Indicates the Ethernet II message. SNAP ether-type <i>type</i> : Indicates the 802.3 SNAP message. LLC dsap <i>value</i> ssap <i>value</i> : Indicates the service access point type of 802.3 LLC message.
Defaults	The protocol VLAN is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The protocol VLAN can be configured on an interface only when the protocol VLAN is globally configured. When the global configuration of a protocol VLAN profile is deleted, the protocol VLAN configuration is deleted from all interfaces corresponding to the profile of the protocol VLAN.

▾ Switching the Port Mode to Trunk/Hybrid Mode

- Mandatory. The protocol VLAN function takes effect only on ports that are in Trunk/Hybrid mode.

▾ Enabling the Protocol VLAN on a Port

- Mandatory. The protocol VLAN is disabled by default.

- The protocol VLAN is truly enabled only when it is applied on interfaces.

Command	protocol-vlan profile num vlan vlan-id
Parameter Description	profile num: Indicates the profile index. vlan vlan-id Indicates the VLAN ID. The value 1 indicates the maximum VLAN ID supported by the product.
Defaults	The protocol VLAN is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	An interface must work in Trunk/Hybrid mode.

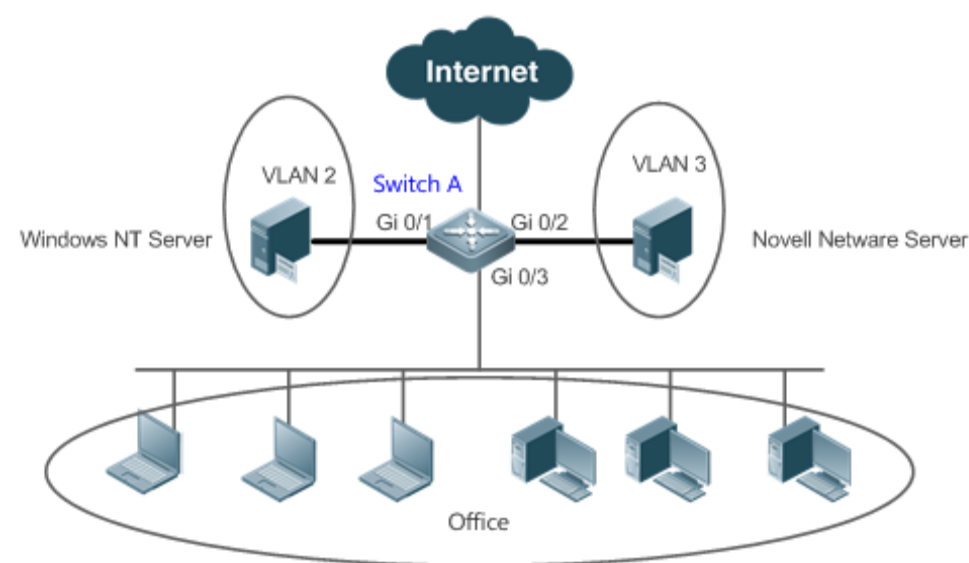
Verification

Run the **show protocol-vlan profile** command to check the configuration.

Configuration Example

Example

Enabling the Protocol VLAN Function in the Topological Environment

<p>Scenario</p> <p>Figure 6-3</p>	 <p>The diagram illustrates a network topology. At the top, a cloud labeled 'Internet' is connected to 'Switch A'. Switch A has three uplink ports: Gi 0/1, Gi 0/2, and Gi 0/3. Gi 0/1 is connected to a 'Windows NT Server' within a circle labeled 'VLAN 2'. Gi 0/2 is connected to a 'Novell Netware Server' within a circle labeled 'VLAN 3'. Gi 0/3 is connected to a horizontal bus that leads to an 'Office' area containing several laptops and servers.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure VLAN 2 and VLAN 3 for user communication on Switch A. ● Configure the protocol VLAN globally on Switch A (in this example, configure Profile 1 for IP protocol packets and configure Profile 2 for IPX protocol packets), enable the protocol VLAN function on the uplink port (Port Gi 0/3 in this example), and complete the protocol-VLAN association (in this example, associate Profile 1 with VLAN 2 and associate Profile 2 with VLAN 3). ● Port Gi 0/1 is an Access port and belongs to VLAN 2. Port Gi 0/2 is also an Access port and belongs to VLAN 3. Port Gi 0/3 is a Hybrid port. Ensure that the user communication VLANs are contained in the permitted untagged VLAN list of the Hybrid port.

<p>A</p>	<p>1. Create VLAN 2 and VLAN 3 for user network communication.</p> <pre>A# configure terminal A(config)# vlan range 2-3</pre> <p>2. Configure the port mode.</p> <pre>A(config)#interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport A(config-if-GigabitEthernet 0/1)#switchport access vlan 2 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#switchport A(config-if-GigabitEthernet 0/2)#switchport access vlan 3 A(config-if-GigabitEthernet 0/2)#exit A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport A(config-if-GigabitEthernet 0/3)# switchport mode hybrid A(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged 2-3</pre> <p>3. Configure the protocol VLAN globally.</p> <p>Configure Profile 1 for IP protocol packets and Profile 2 for IPX protocol packets (in this example, assume that packets are encapsulated using Ethernet II and the Ethernet types of IP protocol packets and IPX protocol packets are 0X0800 and 0X8137 respectively).</p> <pre>A(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800 A(config)#protocol-vlan profile 2 frame-type ETHERII ether-type 0x8137</pre> <p>4. Apply Profile 1 and Profile 2 to Port Gi 0/3 and allocate Profile 1 to VLAN 2 and Profile 2 to VLAN 3.</p> <pre>A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3) #protocol-vlan profile 1 vlan 2 A(config-if-GigabitEthernet 0/3) #protocol-vlan profile 2 vlan 3</pre>
<p>Verification</p>	<p>Check whether the protocol VLAN configuration on the device is correct.</p>
<p>A</p>	<pre>A(config)#show protocol-vlan profile</pre>

profile	frame-type	ether-type/DSAP+SSAP	interface	vlan
1	ETHERII	0x0800	Gi0/3	2
2	ETHERII	0x8137	Gi0/3	3

Common Errors

- A port connected to the device is not in Trunk/Hybrid mode.
- The permitted VLAN list of the port connected to the device does not contain the user communication VLANs.
- The protocol VLAN function is disabled on a port.

6.4.2 Configuring the Subnet VLAN Function

Configuration Effect

Distribute packets from a specified network segment or IP address to a specified VLAN for transmission.

Notes

- It is recommended that the protocol VLAN be configured after VLANs, and the Trunk, Hybrid, Access, and AP attributes of ports are configured.
- If protocol VLAN is configured on a Trunk port or Hybrid port, all VLANs relevant to the protocol VLAN need to be contained in the permitted VLAN list of the Trunk port or Hybrid port.

Configuration Steps

Configuring the Subnet VLAN Globally

- Mandatory.
- The subnet VLAN can be applied on an interface only in global configuration mode.

Command	<code>protocol-vlan ipv4 ip-address mask mask-address vlan vlan-id</code>
Parameter Description	<p>ipv4 ip-addr: Indicates the IP address.</p> <p>mask mask-addr: Indicates the subnet mask.</p> <p>vlan vlan-id: Indicates the VLAN ID. The value 1 indicates the maximum VLAN ID supported by the product.</p>
Defaults	The subnet VLAN is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The subnet VLAN can be enabled on an interface even if the protocol VLAN is not enabled globally. Nevertheless, the subnet VLAN takes effect only when the protocol VLAN is configured globally.

Switching the Port Mode to Trunk/Hybrid Mode

- Mandatory. The subnet VLAN function takes effect only on ports that are in Trunk/Hybrid mode.

Enabling the Subnet VLAN on a Port

- Mandatory. The subnet VLAN is disabled by default.

- The subnet VLAN is truly enabled only when it is applied on interfaces.

Command	protocol-vlan ipv4
Parameter Description	N/A
Defaults	The subnet VLAN is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	An interface must work in Trunk/Hybrid mode.

Verification

Run the **show protocol-vlan ipv4** command to check the configuration.

Configuration

Example

Enabling the Subnet VLAN Function in the Topological Environment

<p>Scenario Figure 6-4</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure VLAN 2 and VLAN 3 for user communication on Switch A. ● Globally configure subnet VLANs on Switch A (in this example, allocate the IP network segment 192.168.1.1/24 to VLAN 3 and the IP network segment 192.168.2.1/24 to VLAN 2) and enable the subnet VLAN function on the uplink port (Port Gi 0/3 in this example). ● Port Gi 0/1 is an Access port and belongs to VLAN 2. Port Gi 0/2 is also an Access port and belongs to VLAN 3. Port Gi 0/3 is a Hybrid port. Ensure that the user communication VLANs are contained in the permitted untagged VLAN list of the Hybrid port.
<p>A</p>	<p>1. Create VLAN 2 and VLAN 3 for user network communication.</p>

	<pre> A# configure terminal A(config)# vlan range 2-3 2. Configure the port mode. A(config)#interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport A(config-if-GigabitEthernet 0/1)#switchport access vlan 2 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#switchport A(config-if-GigabitEthernet 0/2)#switchport access vlan 3 A(config-if-GigabitEthernet 0/2)#exit A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport A(config-if-GigabitEthernet 0/3)# switchport mode hybrid A(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged 2-3 3. Configure the subnet VLAN globally. A(config)# protocol-vlan ipv4 192.168.1.0 mask 255.255.255.0 vlan 3 A(config)# protocol-vlan ipv4 192.168.2.0 mask 255.255.255.0 vlan 2 4. Enable the subnet VLAN on interfaces. The subnet VLAN is disabled by default. (config-if-GigabitEthernet 0/3)# protocol-vlan ipv4 </pre>
Verification	Check whether the subnet VLAN configuration on the device is correct.
A	<pre> A# show protocol-vlan ipv4 ip mask vlan ----- 192.168.1.0 255.255.255.0 3 192.168.2.0 255.255.255.0 2 interface ipv4 status ----- </pre>

Gi0/3	enable
-------	--------

Common Errors


- A port connected to the device is not in Trunk/Hybrid mode.
- The permitted VLAN list of the port connected to the device does not contain the user communication VLANs.
- The subnet VLAN is disabled on a port.

6.5 Monitoring

Displaying

Description	Command
Displays the protocol VLAN content.	show protocol-vlan

Debugging

-  System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the protocol VLAN.	debug bridge protvlan

7 Configuring Private VLAN

7.1 Overview

Private VLAN divides the Layer-2 broadcast domain of a VLAN into multiple subdomains. Each subdomain is composed of one private VLAN pair: primary VLAN and secondary VLAN.

One private VLAN domain may consist of multiple private VLAN pairs and each private VLAN pair represents one subdomain. In a private VLAN domain, all private VLAN pairs share the same primary VLAN. The secondary VLAN IDs of subdomains are different.

If a service provider allocates one VLAN to each user, the number of users that can be supported by the service provider is restricted because one device supports a maximum of 4,096 VLANs. On a Layer-3 device, one subnet address or a series of addresses are allocated to each VLAN, which results in the waste of IP addresses. The private VLAN technology properly solves the preceding two problems. Private VLAN is hereinafter called PVLAN for short.

7.2 Applications

Application	Description
Cross-Device Layer-2 Application of PVLAN	Users of an enterprise can communicate with each other but the user communication between enterprises is isolated.
Layer-3 Application of PVLAN on a Single Device	All enterprise users share the same gateway address and can communicate with the external network.

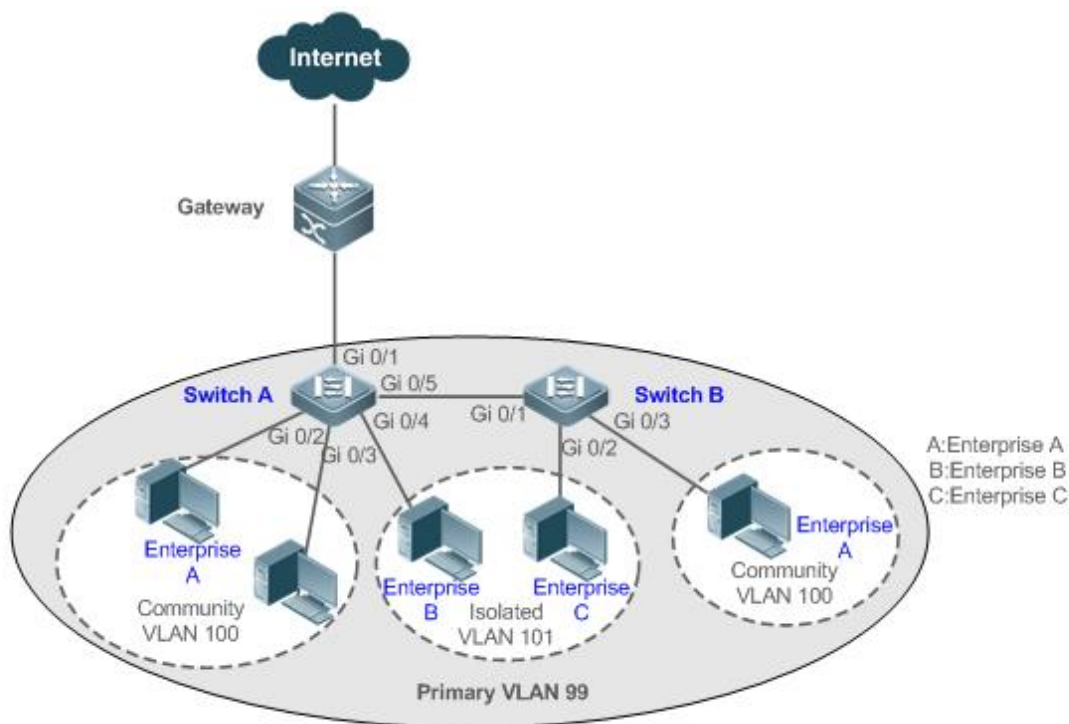
7.2.1 Cross-Device Layer-2 Application of PVLAN

Scenario

As shown in the following figure, in the hosting service operation network, enterprise user hosts are connected to the network through Switch A or Switch B. The main requirements are as follows:

- Users of an enterprise can communicate with each other but the user communication between enterprises is isolated.
- All enterprise users share the same gateway address and can communicate with the external network.

Figure 7-1



Remarks	<p>Switch A and Switch B are access switches.</p> <p>PVLAN runs across devices. The ports for connecting the devices need to be configured as Trunk ports, that is, Port Gi 0/5 of Switch A and Port Gi 0/1 of Switch B are configured as Trunk ports.</p> <p>Port Gi 0/1 for connecting Switch A to the gateway needs to be configured as a promiscuous port.</p> <p>Port Gi 0/1 of the gateway can be configured as a Trunk port or Hybrid port and the Native VLAN is the primary VLAN of PVLAN.</p>
----------------	---

Deployment

- Configure all enterprises to be in the same PVLAN (primary VLAN 99 in this example). All enterprise users share the same Layer-3 interface through this VLAN to communicate with the external network.
- If an enterprise has multiple user hosts, allocate the user hosts of different enterprises to different community VLANs. That is, configure the ports connected to the enterprise user hosts as the host ports of a community VLAN, so as to implement user communication inside an enterprise but isolate the user communication between enterprises.
- If an enterprise has only one user host, configure the ports connected to the user hosts of such enterprises as the host ports of an isolated VLAN so as to implement isolation of user communication between the enterprises.

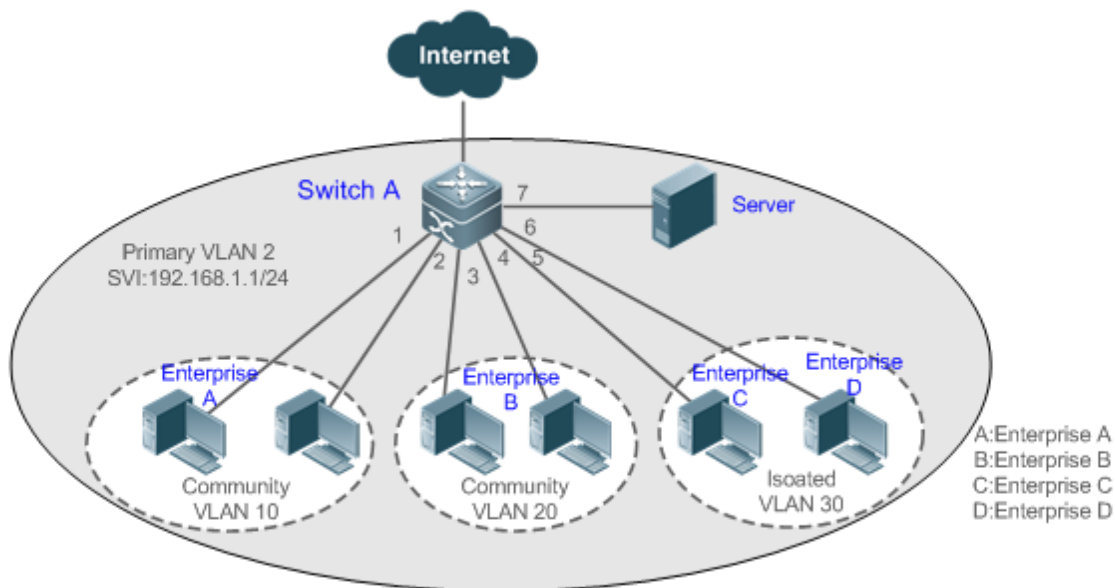
7.2.2 Layer-3 Application of PVLAN on a Single Device

As shown in the following figure, in the hosting service operation network, enterprise user hosts are connected to the network through the Layer-3 device Switch A. The main requirements are as follows:

- Users of an enterprise can communicate with each other but the user communication between enterprises is isolated.

- All enterprise users can access the server.
- All enterprise users share the same gateway address and can communicate with the external network.

Figure 7-2



Remarks	<p>Switch A is a gateway switch.</p> <p>When user hosts are connected to a single device, Port Gi 0/7 for connecting to the server is configured as a promiscuous port so that enterprise users can communicate with the server.</p> <p>Layer-3 mapping needs to be performed on the primary VLAN and secondary VLANs so that the users can communicate with the external network.</p>
----------------	--

Deployment

- Configure the port that is directly connected to the server as a promiscuous port. Then, all enterprise users can communicate with the server through the promiscuous port.
- Configure the gateway address of PVLAN on the Layer-3 device (Switch A in this example) (in this example, set the SVI address of VLAN 2 to 192.168.1.1/24) and configure the mapping between the primary VLAN and secondary VLANs on the Layer-3 interface. Then, all enterprise users can communicate with the external network through the gateway address.

7.3 Features

Basic Concepts

➤ PVLAN

PVLAN supports three types of VLANs: primary VLANs, isolated VLANs, and community VLANs.

A PVLAN domain has only one primary VLAN. Secondary VLANs implement Layer-2 isolation in the same PVLAN domain. There are two types of secondary VLANs.

↘ Isolated VLAN

Ports in the same isolated VLAN cannot mutually make Layer-2 communication. A PVLAN domain has only one isolated VLAN.

↘ Community VLAN

Ports in the same community VLAN can make Layer-2 communication with each other but cannot make Layer-2 communication with ports in other community VLANs. A PVLAN domain can have multiple community VLANs.

↘ Layer-2 Association of PVLAN

PVLAN pairs exist only after Layer-2 association is performed among the three types of VLANs of PVLAN. Then, a primary VLAN has a specified secondary VLAN and a secondary VLAN has a specified primary VLAN. A primary VLAN and secondary VLANs are in the one-to-many relationship.

↘ Layer-3 Association of PVLAN

In PVLAN, Layer-3 interfaces, that is, switched virtual interfaces (SVIs) can be created only in a primary VLAN. Users in a secondary VLAN can make Layer-3 communication only after Layer-3 association is performed between the secondary VLAN and the primary VLAN. Otherwise, the users can make only Layer-2 communication.

↘ Isolated Port

A port in an isolated VLAN can communicate only with a promiscuous port. An isolated port can forward the received packets to a Trunk port but a Trunk port cannot forward the packets with the VID of an isolated VLAN to an isolated port.

↘ Community Port

Community ports are ports in a community VLAN. Community ports in the same community VLAN can communicate with each other and can communicate with promiscuous ports. They cannot communicate with community ports in other community VLANs or isolated ports in an isolated VLAN.

↘ Promiscuous Port

Promiscuous ports are ports in a primary VLAN. They can communicate with any ports, including isolated ports and community ports in secondary VLANs of the same PVLAN domain.

↘ Promiscuous Trunk Port

A promiscuous Trunk port is a member port that belongs to multiple common VLANs and multiple PVLANS at the same time. It can communicate with any ports in the same VLAN.

- In a common VLAN, packet forwarding complies with 802.1Q.
- In PVLAN, for tagged packets to be forwarded by a promiscuous Trunk port, if the VID of the packets is a secondary VLAN ID, the VID is converted into the corresponding primary VLAN ID before packet forwarding.

↘ Isolated Trunk Port

An isolated Trunk port is a member port that belongs to multiple common VLANs and multiple PVLANS at the same time.

- In an isolated VLAN, an isolated Trunk port can communicate only with a promiscuous port.

- In a community VLAN, an isolated Trunk port can communicate with community ports in the same community VLAN and promiscuous ports.
- In a common VLAN, packet forwarding complies with 802.1Q.
- An isolated Trunk port can forward the received packets of an isolated VLAN ID to a Trunk port but a Trunk port cannot forward the packets with the VID of an isolated VLAN to an isolated port.
- For tagged packets to be forwarded by an isolated Trunk port, if the VID of the packets is a primary VLAN ID, the VID is converted into a secondary VLAN ID before packet forwarding.

- ⚠ In PVLAN, SVIs can be created only in a primary VLAN and SVIs cannot be created in secondary VLANs.
- ⚠ Ports in PVLAN can be used as mirroring source ports but cannot be used as mirroring destination ports.

Overview

Feature	Description
PVLAN Layer-2 Isolation and IP Address Saving	Ports of different PVLAN types can be configured to implement interworking and isolation of VLAN intermediate user hosts.
	After Layer-2 mapping is performed between a primary VLAN and secondary VLANs, only Layer-2 communication is supported. If Layer-3 communication is required, users in a secondary VLAN need to use SVIs of the primary VLAN to make Layer-3 communication.

7.3.1 PVLAN Layer-2 Isolation and IP Address Saving

Add users to subdomains of PVLAN to isolate communication between enterprises and between enterprise users.

Working Principle

Configure PVLAN, configure Layer-2 association and Layer-3 association between a primary VLAN and SubVLANs of PVLAN, and configure ports connected to user hosts, external network devices, and servers as different types of PVLAN ports. In this way, subdomain division and communication of users in subdomains with the external network and servers can be implemented.

Packet Forwarding Relationship Between Ports of Different Types

Output Port \ Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Port (in the Same VLAN)	Trunk Same	Promiscuous Trunk Port (in the Same VLAN)	Trunk Port (in the Same VLAN)
Promiscuous Port	Supported	Supported	Supported	Supported		Supported	Supported
Isolated Port	Supported	Unsupported	Unsupported	Unsupported		Supported	Supported
Community Port	Supported	Unsupported	Supported	Supported		Supported	Supported
Isolated Trunk Port (in the Same)	Supported	Unsupported	Supported	Unsupported (unsupported in an isolated VLAN but supported in a		Supported	Supported





Output Port Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (in the Same VLAN)	Promiscuous Trunk Port (in the Same VLAN)	Trunk Port (in the Same VLAN)
VLAN)				non-isolated VLAN)		
Promiscuous Trunk Port (in the Same VLAN)	Supported	Supported	Supported	Supported	Supported	Supported
Trunk Port (in the Same VLAN)	Supported	Unsupported	Supported	Unsupported (unsupported in an isolated VLAN but supported in a non-isolated VLAN)	Supported	Supported


▾ VLAN Tag Changes After Packet Forwarding Between Ports of Different Types

Output Port Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (in the Same VLAN)	Promiscuous Trunk Port (in the Same VLAN)	Trunk Port (in the Same VLAN)
Promiscuous Port	Unchanged	Unchanged	Unchanged	A secondary VLAN ID is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	A primary VLAN ID tag is added.
Isolated Port	Unchanged	NA	NA	NA	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	An isolated VLAN ID tag is added.
Community Port	Unchanged	NA	Unchanged	A community VLAN ID tag is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	A community VLAN ID tag is added.
Isolated Trunk Port (in the Same VLAN)	The VLAN tag is removed.	NA	The VLAN tag is removed.	The VLAN tag keeps unchanged in a non-isolated VLAN.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the	Unchanged

Output Port Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (in the Same VLAN)	Promiscuous Trunk Port (in the Same VLAN)	Trunk Port (in the Same VLAN)
					non-PVLAN.	
Promiscuous Trunk Port (in the Same VLAN)	The VLAN tag is removed.	Unchanged	Unchanged	A secondary VLAN ID is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	Unchanged
Trunk Port (in the Same VLAN)	The VLAN tag is removed.	NA	The VLAN tag is removed.	The VLAN tag is converted into a secondary VLAN ID in a primary VLAN and the VLAN tag keeps unchanged in other non-isolated VLANs.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	Unchanged
Switch CPU	Untag	Untag	Untag	A secondary VLAN ID tag is added.	A primary VLAN ID tag is added and the VLAN tag keeps unchanged in the non-PVLAN.	A primary VLAN ID tag is added.

7.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of PVLAN	 (Mandatory) It is used to configure a primary VLAN and secondary VLANs.	
	private-vlan { community isolated primary }	Configures the PVLAN type.
	 (Mandatory) It is used to configure Layer-2 association between a primary VLAN and secondary VLANs of PVLAN to form PVLAN pairs.	
	private-vlan association { svlist add svlist remove svlist }	Configures Layer-2 association between a primary VLAN and secondary VLANs to form PVLAN pairs.
	 (Optional) It is used to allocate users to an isolated VLAN or community VLAN.	
	switchport mode private-vlan host	Configures a PVLAN host port.
	switchport private-vlan host-association p_vid s_vid	Associates Layer-2 ports with PVLAN and allocates ports to subdomains.
 (Optional) It is used to configure a port as a promiscuous port.		

Configuration	Description and Command	
	Switchport mode private-vlan promiscuous	Configures a PVLAN promiscuous port.
	switchport private-vlan mapping <i>p_vid</i> { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	Configures the primary VLAN to which a PVLAN promiscuous port belongs and a list of secondary VLANs. PVLAN packets can be transmitted or received through this port only after the configuration is performed.
	 (Optional) It is used to configure Layer-3 communication for users in a secondary VLAN.	
	private-vlan mapping { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	Configures the SVI of the primary VLAN and configures Layer-3 association between the primary VLAN and secondary VLANs after PVLAN is created and Layer-2 association is performed. Users in a SubVLAN can make Layer-3 communication through the SVI of the primary VLAN.

7.4.1 Configuring Basic Functions of PVLAN

Configuration Effect

- Enable PVLAN subdomains to form to implement isolation between enterprises and between enterprise users.
- Implement Layer-3 mapping between multiple secondary VLANs and the primary VLAN so that and multiple VLANs uses the same IP gateway, thereby helping save IP addresses.

Notes

- After a primary VLAN and a secondary VLAN are configured, a PVLAN subdomain exist only after Layer-2 association is performed between them.
- A port connected to a use host must be configured as a specific PVLAN port so that the user host joins a subdomain to implement the real user isolation.
- The port connected to the external network and the port connected to a server must be configured as promiscuous ports so that upstream and downstream packets are forwarded normally.
- Users in a secondary VLAN can make Layer-3 communication through the SVI of the primary VLAN only after Layer-3 mapping is performed between the secondary VLAN and the primary VLAN.

Configuration Steps

↘ Configuring PVLAN

- Mandatory.
- A primary VLAN and a secondary VLAN must be configured. The two types of VLANs cannot exist independently.
- Run the **private-vlan { community | isolated | primary }** command to configure a VLAN as the primary VLAN of PVLAN and other VLANs as secondary VLANs.

Command	private-vlan { community isolated primary }
----------------	--

Parameter Description	<p>community: Specifies that the VLAN type is community VLAN.</p> <p>isolated: Specifies that the VLAN type is isolated VLAN.</p> <p>primary: Specifies that the VLAN type is the primary VLAN of a PVLAN pair.</p>
Defaults	VLANs are common VLANs and do not have the attributes of PVLAN.
Command Mode	VLAN mode
Usage Guide	This command is used to specify the primary VLAN and secondary VLANs of PVLAN.

↘ Configuring Layer-2 Association of PVLAN

- Mandatory.
- PVLAN subdomains form, and isolated ports, community ports, and Layer-3 association can be configured only after Layer-2 association is performed between the primary VLAN and secondary VLANs of PVLAN.
- By default, after various PVLANS are configured, the primary VLANs and secondary VLANs are independent of each other. A primary VLAN has a secondary VLAN and a secondary VLAN has a primary VLAN only after Layer-2 association is performed.
- Run the **private-vlan association { svlist | add svlist | remove svlist }** command to configure or cancel the Layer-2 association between the primary VLAN and secondary VLANs of PVLAN. A PVLAN subdomain forms only after Layer-2 association is configured,. The PVLAN subdomain does not exist after Layer-2 association is cancelled. If Layer-2 association is not performed, when isolated ports and promiscuous ports are used to configure associated PVLAN pairs, the configuration will fail or the association between ports and VLANs will be cancelled.

Command	private-vlan association { svlist add svlist remove svlist }
Parameter Description	<p><i>svlist</i>: Specifies the list of secondary VLANs to be associated or disassociated.</p> <p>add svlist: Adds the secondary VLANs to be associated.</p> <p>remove svlist: Cancels the association between <i>svlist</i> and the primary VLAN.</p>
Defaults	By default, the primary VLAN and secondary VLANs are not associated.
Command Mode	Primary VLAN mode of PVLAN
Usage Guide	<p>This command is used to configure Layer-2 association between a primary VLAN and secondary VLANs to form PVLAN pairs.</p> <p>Each primary VLAN can be associated with only one isolated VLAN but can be associated with multiple community VLANs.</p>

↘ Configuring Layer-3 Association of PVLAN

- If users in a secondary VLAN domain need to make Layer-3 communication, configure a Layer-3 interface SVI for the primary VLAN and then configure Layer-3 association between the primary VLAN and secondary VLANs on the SVI.
- By default, SVIs can be configured only in a primary VLAN. Secondary VLANs do not support Layer-3 communication.

- If users in a secondary VLAN of PVLAN need to make Layer-3 communication, the SVI of the primary VLAN needs to be used to transmit and receive packets.
- Run the **private-vlan mapping** { *svlist* | **add** *svlist* | **remove** *svlist* } command to configure or cancel the Layer-3 association between the primary VLAN and secondary VLANs of PVLAN. Users in a secondary VLAN can make Layer-3 communication with the external network only after Layer-3 association is configured. After Layer-3 association is cancelled, users in a secondary VLAN cannot make Layer-3 communication.

Command	private-vlan mapping { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }
Parameter Description	<i>svlist</i> : Indicates the list of secondary VLANs, for which Layer-3 mapping needs to be configured. add <i>svlist</i> : Adds the secondary VLANs to be associated with a Layer-3 interface. remove <i>svlist</i> : Cancels the secondary VLANs associated with a Layer-3 interface.
Defaults	By default, the primary VLAN and secondary VLANs are not associated.
Command Mode	Interface configuration mode of the primary VLAN
Usage Guide	A Layer-3 SVI must be configured for the primary VLAN first. Layer-3 interfaces can be configured only in a primary VLAN. Layer-2 association must be performed between associated secondary VLANs and the primary VLAN.

↘ **Configuring Isolated Ports and Community Ports**

- After the primary VLAN and secondary VLANs of PVLAN as well as Layer-2 association are configured, allocate the device ports connected to user hosts so as to specify the subdomains to which the user hosts belong.
- If an enterprise has only one user host, set the port connected to the user host as an isolated port.
- If an enterprise has multiple user hosts, set the ports connected to the user hosts as community ports.

Command	switchport mode private-vlan host switchport private-vlan host-association <i>p_vid</i> <i>s_vid</i>
Parameter Description	<i>p_vid</i> : Indicates the primary VLAN ID in a PVLAN pair. <i>s_vid</i> : Indicates the secondary VLAN ID in a PVLAN pair. The port is an associated port if the VLAN is an isolated VLAN and the port is a community port if the VLAN is a community VLAN.
Defaults	By default, the interface works in Access mode; no private VLAN pairs are associated.
Command Mode	Both commands run in interface configuration mode.
Usage Guide	Both the preceding commands need to be configured. Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode. Whether a port is configured as an isolated port or community port depends on the <i>s_vid</i> parameter. <i>p_vid</i> and <i>s_vid</i> must be respectively the IDs of the primary VLAN and secondary VLAN in a PVLAN pair, on which Layer-2 association is performed. One host port can be associated with only one PVLAN pair.

↘ **Configuring a Promiscuous Port**

- According to the table listing port packet transmission and receiving rules in section "Features", the single port type of PVLAN cannot ensure symmetric forwarding of upstream and downstream packets. Ports for connecting to

the external network or server need to be configured as promiscuous ports to ensure that users can successfully access the external network or server.

Command	switchport mode private-vlan promiscuous switchport private-vlan mapping <i>p_vid</i> { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }
Parameter Description	<i>p_vid</i> : Indicates the primary VLAN ID in a PVLAN pair. <i>svlist</i> : Indicates the secondary VLAN associated with a promiscuous port. Layer-2 association must be performed between it and <i>p_vid</i> . add <i>svlist</i> : Adds a secondary VLAN to be associated with a port. remove <i>svlist</i> : Cancels the secondary VLAN associated with a port.
Defaults	By default, an interface works in Access mode; a promiscuous port is not associated with a secondary VLAN.
Command Mode	Interface configuration mode
Usage Guide	The port mode must be configured as the promiscuous mode. If a port is configured as a promiscuous port, it must be associated with PVLN pairs. Otherwise, the port cannot bear or forward services. One promiscuous port can be associated with multiple PVLAN pairs within one primary VLAN but cannot be associated with multiple primary VLANs.

Verification

Make user hosts connected to PVLAN ports transmit and receive packets as per PVLAN port forwarding rules to implement isolation. Configure Layer-3 association to make users in the primary VLAN and secondary VLANs of the same PVLAN to share the same gateway IP address and make Layer-3 communication.

Configuration

Example

↘ Cross-Device Layer-2 Application of PVLAN

<p>Figure 7-3</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure all enterprises to be in the same PVLAN (primary VLAN 99 in this example). All enterprise users share the same Layer-3 interface through this VLAN to communicate with the external network. ● If an enterprise has multiple user hosts, allocate each enterprise to a different community VLAN (in this example, allocate Enterprise A to Community VLAN 100) to implement user communication inside an enterprise and isolate user communication between enterprises. ● If an enterprise has only one user host, allocate such enterprises to the same isolated VLAN (in this example, allocate Enterprise B and Enterprise C to Isolated VLAN 101) to isolate user communication between enterprises.
<p>Switch A</p>	<pre> SwitchA# configure terminal SwitchA(config)# vlan 99 SwitchA(config-vlan)# private-vlan primary SwitchA(config-vlan)# exit SwitchA(config)# vlan 100 SwitchA(config-vlan)# private-vlan community SwitchA(config-vlan)# exit SwitchA(config)# vlan 101 SwitchA(config-vlan)# private-vlan isolated SwitchA(config-vlan)# exit SwitchA(config)# vlan 99 SwitchA(config-vlan)# private-vlan association 100-101 SwitchA(config-vlan)# exit SwitchA(config)# interface range gigabitEthernet 0/2-3 SwitchA(config-if-range)# switchport mode private-vlan host SwitchA(config-if-range)# switchport private-vlan host-association 99 100 SwitchA(config-if-range)# exit </pre>

	<pre>SwitchA(config)# interface gigabitEthernet 0/4 SwitchA(config-if-GigabitEthernet 0/4)# switchport mode private-vlan host SwitchA(config-if-GigabitEthernet 0/4)# switchport private-vlan host-association 99 101 SwitchA(config)# interface gigabitEthernet 0/5 SwitchA(config-if-GigabitEthernet 0/5)# switchport mode trunk SwitchA(config-if-GigabitEthernet 0/5)# exit</pre>
Switch B	<pre>SwitchB# configure terminal SwitchB(config)# vlan 99 SwitchB(config-vlan)# private-vlan primary SwitchB(config-vlan)# exit SwitchB(config)# vlan 100 SwitchB(config-vlan)# private-vlan community SwitchB(config-vlan)# exit SwitchB(config)# vlan 101 SwitchB(config-vlan)# private-vlan isolated SwitchB(config-vlan)# exit SwitchB(config)# vlan 99 SwitchB(config-vlan)# private-vlan association 100-101 SwitchB(config-vlan)# exit SwitchB(config)# interface gigabitEthernet 0/2 SwitchB(config-if-GigabitEthernet 0/2)# switchport mode private-vlan host SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan host-association 99 101 SwitchB(config-if-GigabitEthernet 0/2)# exit SwitchB(config)# interface gigabitEthernet 0/3 SwitchB(config-if-GigabitEthernet 0/3)# switchport mode private-vlan host SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan host-association 99 100 SwitchB(config-if-GigabitEthernet 0/3)# exit SwitchB(config)# interface gigabitEthernet 0/1 SwitchB(config-if-GigabitEthernet 0/1)# switchport mode trunk SwitchB(config-if-GigabitEthernet 0/1)# exit</pre>
Verification	Check whether VLANs and ports are correctly configured, and check whether packet forwarding is correct according to packet forwarding rules in section "Features".
Switch A	<pre>SwitchA# show running-config ! vlan 99 private-vlan primary private-vlan association add 100-101 ! vlan 100 private-vlan community ! vlan 101 private-vlan isolated</pre>


```

!
interface GigabitEthernet 0/1
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 99 add 100-101
!
interface GigabitEthernet 0/2
  switchport mode private-vlan host
  switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/3
  switchport mode private-vlan host
  switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/4
  switchport mode private-vlan host
  switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/5
  switchport mode trunk
!
SwitchA# show vlan private-vlan
VLAN  Type      Status  Routed  Ports          Associated VLANs
-----
99    primary   active  Disabled Gi0/1, Gi0/5    100-101
100   community active  Disabled Gi0/2, Gi0/3, Gi0/5    99
101   isolated  active  Disabled Gi0/4, Gi0/5     99

```

Switch B

```

SwitchB# show running-config
!
vlan 99
  private-vlan primary
  private-vlan association add 100-101
!
vlan 100
  private-vlan community
!
vlan 101
  private-vlan isolated
!
interface GigabitEthernet 0/1
  switchport mode trunk
!
interface GigabitEthernet 0/2
  switchport mode private-vlan host
  switchport private-vlan host-association 99 101

```

```
!
interface GigabitEthernet 0/3
  switchport mode private-vlan host
  switchport private-vlan host-association 99 100
```

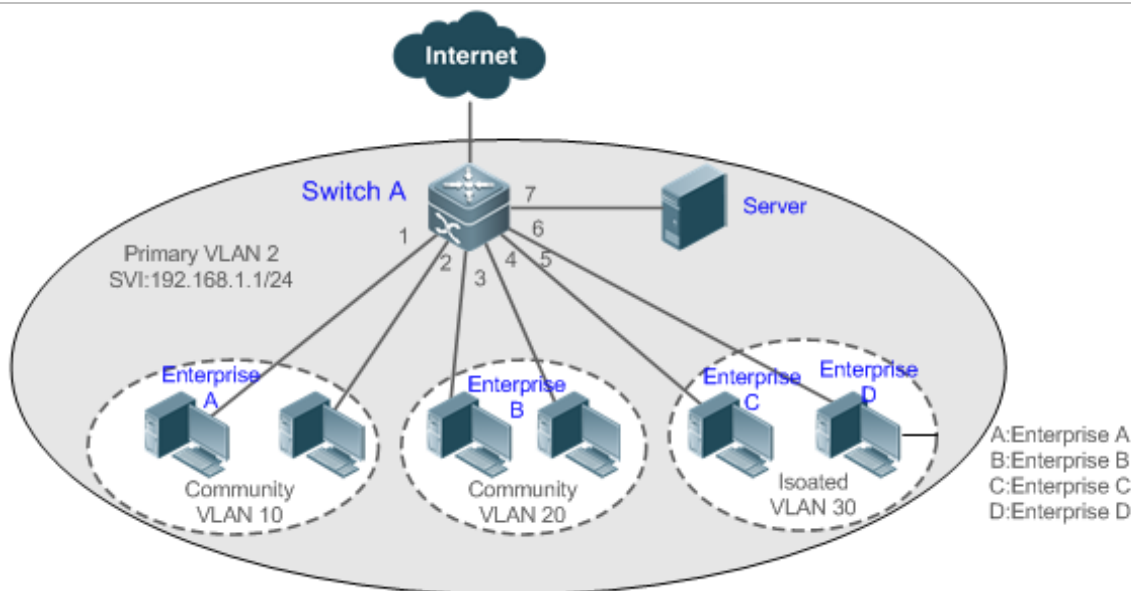
Common Errors

- Layer-2 association is not performed between the primary VLAN and secondary VLANs of PVLAN, and a port VLAN list fails to be added when isolated ports, promiscuous ports, and community ports are configured.
- One host port fails to be associated with multiple PVLAN pairs.

Configuration Example

Layer-3 Application of PVLAN on a Single Device

Figure 7-4



Configuration Steps

- Configure the PVLAN function on the device (Switch A in this example). For details about the configuration, see configuration tips in "Cross-Device Layer-2 Application of PVLAN."
- Set the port that is directly connected to the server (Port Gi 0/7 in this example) as a promiscuous port. Then, all enterprise users can communicate with the server through the promiscuous port.
- Configure the gateway address of PVLAN on the Layer-3 device (Switch A in this example) (in this example, set the SVI address of VLAN 2 to 192.168.1.1/24) and configure the Layer-3 interface mapping between the primary VLAN (VLAN 2 in this example) and secondary VLANs (VLAN 10, VLAN 20, and VLAN 30 in this example). Then, all enterprise users can communicate with the external network through the gateway address.

! Run PVLAN cross devices and configure the ports for connecting to the devices as Trunk ports.

Switch A

```
SwitchA# configure terminal
SwitchA(config)# vlan 2
SwitchA(config-vlan)# private-vlan primary
```

```
SwitchA(config-vlan)# exit
SwitchA(config)# vlan 10
SwitchA(config-vlan)# private-vlan community
SwitchA(config-vlan)# exit
SwitchA(config)# vlan 20
SwitchA(config-vlan)# private-vlan community
SwitchA(config-vlan)# exit
SwitchA(config)# vlan 30
SwitchA(config-vlan)# private-vlan isolated
SwitchA(config-vlan)# exit
SwitchA(config)# vlan 2
SwitchA(config-vlan)# private-vlan association 10,20,30
SwitchA(config-vlan)# exit
SwitchA(config)# interface range gigabitEthernet 0/1-2
SwitchA(config-if-range)# switchport mode private-vlan host
SwitchA(config-if-range)# switchport private-vlan host-association 2 10
SwitchA(config-if-range)# exit
SwitchA(config)# interface range gigabitEthernet 0/3-4
SwitchA(config-if-range)# switchport mode private-vlan host
SwitchA(config-if-range)# switchport private-vlan host-association 2 20
SwitchA(config-if-range)# exit
SwitchA(config)# interface range gigabitEthernet 0/5-6
SwitchA(config-if-range)# switchport mode private-vlan host
SwitchA(config-if-range)# switchport private-vlan host-association 2 30
SwitchA(config-if-range)# exit
SwitchA(config)# interface gigabitEthernet 0/7
SwitchA(config-if-GigabitEthernet 0/7)# switchport mode private-vlan promiscuous
SwitchA(config-if-GigabitEthernet 0/7)# switchport private-vlan mapping 2 10,20,30
SwitchA(config-if-GigabitEthernet 0/7)# exit
SwitchA(config)# interface vlan 2
SwitchA(config-if-VLAN 2)# ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 2)# private-vlan mapping 10,20,30
SwitchA(config-if-VLAN 2)# exit
```

Verification	Ping the gateway address 192.168.1.1 from user hosts in different subdomains. The ping operation is successful.
Switch A	<pre>SwitchA#show running-config ! vlan 2 private-vlan primary private-vlan association add 10,20,30 ! vlan 10 private-vlan community ! vlan 20 private-vlan community ! vlan 30 private-vlan isolated ! interface GigabitEthernet 0/1 switchport mode private-vlan host switchport private-vlan host-association 2 10 ! interface GigabitEthernet 0/2 switchport mode private-vlan host switchport private-vlan host-association 2 10 ! interface GigabitEthernet 0/3 switchport mode private-vlan host switchport private-vlan host-association 2 20 ! interface GigabitEthernet 0/4 switchport mode private-vlan host switchport private-vlan host-association 2 20 !</pre>

```

interface GigabitEthernet 0/5
  switchport mode private-vlan host
  switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
  switchport mode private-vlan host
  switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
  no ip proxy-arp
  ip address 192.168.1.1 255.255.255.0
  private-vlan mapping add 10,20,30
!
SwitchA#show vlan private-vlan
VLAN  Type   Status  Routed  Ports  Associated VLANs
-----
2     primary  active  Enabled  Gi0/7   10,20,30
10    community active  Enabled  Gi0/1, Gi0/2  2
20    community active  Enabled  Gi0/3, Gi0/4  2
30    isolated active  Enabled  Gi0/5, Gi0/6  2

```

Common Errors


- No Layer-2 association is performed on the primary VLAN and secondary VLANs of PVLAN and the Layer-3 association fails to be configured.
- The device is connected to the external network before Layer-3 association is configured. As a result, the device cannot communicate with the external network.
- The interfaces for connecting to the server and the external network are not configured as promiscuous interfaces, which results in asymmetric forwarding of upstream and downstream packets.

7.5 Monitoring

Displaying

Description	Command
Displays PVLAN configuration.	show vlan private-vlan [community primary isolated]

Debugging

-  System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs PVLAN.	debug bridge pvlan

8 Configuring Voice VLAN

8.1 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.

8.2 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.

8.2.1 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 8-1 Networking When the Voice VLAN Works in Automatic Mode



The Gi0/1 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 Gi0/1 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.

- i** 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

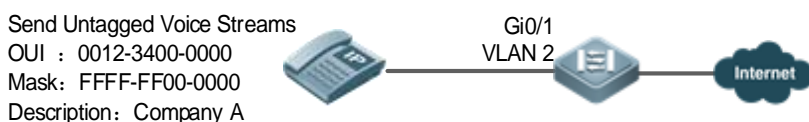
- Enable the port connected to IP phones to work in automatic mode and send tagged voice streams to devices.

8.2.2 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 8-2 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 Gi0/1 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 Gi0/1 port is configured as a hybrid port. According to the matching relationship requirement (see "Features"), the native VLAN of the Gi0/1 port must be a voice VLAN, and the voice VLAN must be added to the allowed untagged VLAN list of the port.

Deployment

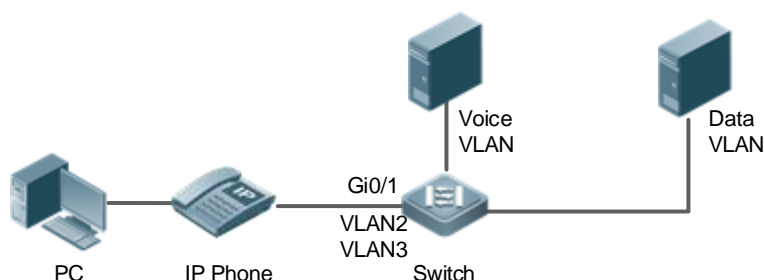
- Enable the port connected to IP phones to work in manual mode and send untagged voice streams to devices.

8.2.3 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 8-3 Networking That Isolates Voice Streams from Data Streams



The Gi0/1 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 Gi0/1 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 Gi0/1 port. The native VLAN of the Gi0/1 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.

8.3 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, delivers a policy to change the CoS priority and the DSCP priority of voice packets to **6** and **46** respectively, 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 delivers a policy to change the CoS priority and the DSCP priority of voice packets to **6** and **46** respectively.

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:

4. The IP phone automatically obtains an IP address, but not the voice VLAN information.
5. 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


Working Mode of the Voice VLAN	Voice Stream Type	Port Type	Supported Or Not
			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.
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.


Working Mode of the Voice VLAN	Voice Stream Type	Port Type	Supported Or Not
	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.
		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.

8.3.1 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 improves the priority of voice packets to 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.

8.4 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	 (Optional) It is used to configure the aging time of the voice VLAN.	

Configuration Item	Description and Command	
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 Voice VLAN	⚠ (Optional) It is used to configure the OUI of the 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 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.

8.4.1 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 <i>vlan-id</i>
Parameter	<i>vlan-id</i> : Indicates the ID of a VLAN. The value ranges from 2 to 4,094.
Description	
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.

i 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 Ruijie 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	N/A
Description	
Command Mode	All configuration modes
Usage Guide	N/A
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Current voice VLAN enabled port mode: PORT MODE -----</pre>

Configuration

Example

Configuring a Voice VLAN

Configuration Steps	<ul style="list-style-type: none"> ● Create VLAN 2. ● Globally enable the voice VLAN function, and configure VLAN 2 as a voice VLAN.
	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# vlan 2 Ruijie(config-vlan)# exit Ruijie(config)# voice vlan 2</pre>
Verification	Run the show voice vlan command to check whether the configuration is correct.
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE</pre>

	Voice VLAN ID : 2
	Voice VLAN security mode: Security
	Voice VLAN aging time : 1440 minutes
	Current voice VLAN enabled port mode:
	PORT MODE

8.4.2 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	N/A
Description	
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	N/A
Description	
Command Mode	All configuration modes

Usage Guide	N/A
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Current voice VLAN enabled port mode: PORT MODE ----- Gi0/1 MANUAL</pre>

Configuration Example

▾ Enabling the Voice VLAN Function on a Port

Configuration Steps	<ul style="list-style-type: none"> Enter the port configuration mode, and enable the voice VLAN function on a physical port.
	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if)# voice vlan enable</pre>
Verification	Run the show voice vlan command to check whether the configuration is correct.
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Current voice VLAN enabled port mode: PORT MODE ----- Gi0/1 MANUAL</pre>

8.4.3 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 <i>minutes</i>
Parameter Description	<i>minute</i> : Indicates the aging time of the voice VLAN.
Defaults	By default, the aging time is 1,440 minutes.
Command Mode	Global configuration 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
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Current voice VLAN enabled port mode: PORT MODE -----</pre>

Configuration

Example

Configuring the Aging Time of the Voice VLAN

Configuration Steps	<ul style="list-style-type: none"> ● Set the aging time of the voice VLAN to 10 minutes.
	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# voice vlan aging 10</pre>
Verification	Run the show voice vlan command to check whether the configuration is correct.
	<pre>Ruijie#show voice vlan</pre>

Voice VLAN status	: ENABLE
Voice VLAN ID	: 10
Voice VLAN security mode:	Security
Voice VLAN aging time	: 10 minutes
Current voice VLAN enabled port mode:	
PORT	MODE
-----	-----

8.4.4 Configuring the OUI of the Voice VLAN

Configuration Effect

- Ruijie 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 <i>mac-addr</i> mask <i>oui-mask</i> [description <i>text</i>]
Parameter	<i>mac-addr</i> : Indicates the source MAC address in a voice packet.
Description	<i>oui-mask</i> : Indicates the valid length of the OUI, which is expressed by a mask. <i>text</i> : 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	N/A
Description	
Command Mode	All configuration modes
Usage Guide	N/A

Ruijie(config)# show voice vlan oui								
<table border="1"> <thead> <tr> <th>Oui</th> <th>Address</th> <th>Mask</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0012.3400.0000</td> <td>ffff.ff00.0000</td> <td></td> <td>Company A</td> </tr> </tbody> </table>	Oui	Address	Mask	Description	0012.3400.0000	ffff.ff00.0000		Company A
Oui	Address	Mask	Description					
0012.3400.0000	ffff.ff00.0000		Company A					

Configuration

Example

▾ Configuring the OUI of the Voice VLAN

Configuration Steps	<ul style="list-style-type: none"> Set the OUI of the voice VLAN to 0012.3400.0000, and the supplier is Company A. 								
	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000 description Company A</pre>								
Verification	Run the show voice vlan oui command to check whether the configuration is correct.								
	<pre>Ruijie(config)# show voice vlan oui</pre> <table border="1"> <thead> <tr> <th>Oui</th> <th>Address</th> <th>Mask</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0012.3400.0000</td> <td>ffff.ff00.0000</td> <td></td> <td>Company A</td> </tr> </tbody> </table>	Oui	Address	Mask	Description	0012.3400.0000	ffff.ff00.0000		Company A
Oui	Address	Mask	Description						
0012.3400.0000	ffff.ff00.0000		Company A						

8.4.5 Configuring the Security Mode of the Voice VLAN

Configuration Effect

- To better isolate voice streams from data streams during transmission, Ruijie 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	N/A
Description	
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
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Current voice VLAN enabled port mode: PORT MODE -----</pre>

Configuration

Example

▾ Configuring the Security Mode of the Voice VLAN

Configuration Steps	<ul style="list-style-type: none"> ● Enter the global configuration mode, and enable the security mode of the voice VLAN.
	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# voice vlan security enable</pre>
Verification	Run the show voice vlan command to check whether the configuration is correct.
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security Voice VLAN aging time : 1440 minutes Current voice VLAN enabled port mode: PORT MODE -----</pre>

8.4.6 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 a Ruijie 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	N/A
Description	
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.

- i** 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.
- i** 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	N/A
Description	
Command Mode	All configuration modes
Usage Guide	N/A
	<pre>Ruijie#show voice vlan Voice VLAN status : ENABLE Voice VLAN ID : 10 Voice VLAN security mode: Security</pre>

Voice VLAN aging time	: 1440 minutes
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

<p>Scenario Figure 8-4</p>	 <p>Send Tagged Voice Streams OUI : 0012-3400-0000 Mask: FFFF-FF00-0000 Description: Company A</p>
<p>Configuration Steps</p>	<p>Configuration Tips</p> <ul style="list-style-type: none"> The Gi0/1 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 Gi0/1 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 Gi0/1 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 Gi0/1 port.
	<p>Step 1: Create VLAN 2, and configure this VLAN as the voice VLAN.</p> <pre>Ruijie# configure terminal Ruijie(config)# vlan 2 Ruijie(config-vlan)# exit Ruijie(config)# voice vlan 2</pre> <p>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.</p> <pre>Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000</pre> <p>Step 3: Configure Gi0/1 as the trunk port, and VLAN 5 as the native VLAN of the port.</p>


	<pre>Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if)# switchport mode trunk Ruijie(config-if)# switchport trunk native vlan 5</pre> <p>Step 4: Delete the voice VLAN from the allowed VLAN list of the Gi0/1 port, and enable the voice VLAN function of the Gi0/1 port.</p> <pre>Ruijie(config-if)# switchport trunk allowed vlan remove 2 Ruijie(config-if)# voice vlan enable</pre>
Verification	<ul style="list-style-type: none"> Run the show voice vlan command to check the current status of the voice VLAN on the device.
	<pre>Ruijie(config)# show voice vlan Voice Vlan status: ENABLE Voice Vlan ID : 2 Voice Vlan security mode: Security Voice Vlan aging time: 1440 minutes Current voice vlan enabled port mode: PORT MODE ----- Gi0/1 AUTO # Check Voice VLAN OUI Address Ruijie(config)# show voice vlan oui Oui Address Mask Description 0012.3400.0000 ffff.ff00.0000</pre>

8.5 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

9 Configuring VLAN Mapping

9.1 Overview

VLAN mapping enables cross-VLAN communication by converting VLAN IDs between the two different networks. The common scenarios are as below:

1. Deployment of two networks is not symmetrical
2. VLAN ID conflicts in the new and old networks.

By modifying instead of adding VLAN tags, VLAN mapping requires two prerequisites:

- Both users are in the same network segment. VLAN mapping is a Layer-2 based function. However, communication in different network segments requires Layer-3 function, which cannot be implemented by VLAN mapping.
- The packets received by the provider edge device need to carry tags. Therefore, the packets sent from the uplink port of the customer edge device should be tagged.

9.2 Applications

Application	Description
Implementing VLAN Aggregation for Different Services Through VLAN Mapping	Different service flows (PC, IPTV, and VoIP) are transmitted through different VLANs. The VLANs are aggregated on a campus network so that only one VLAN is used to carry the same service flows, thus saving VLAN resources.

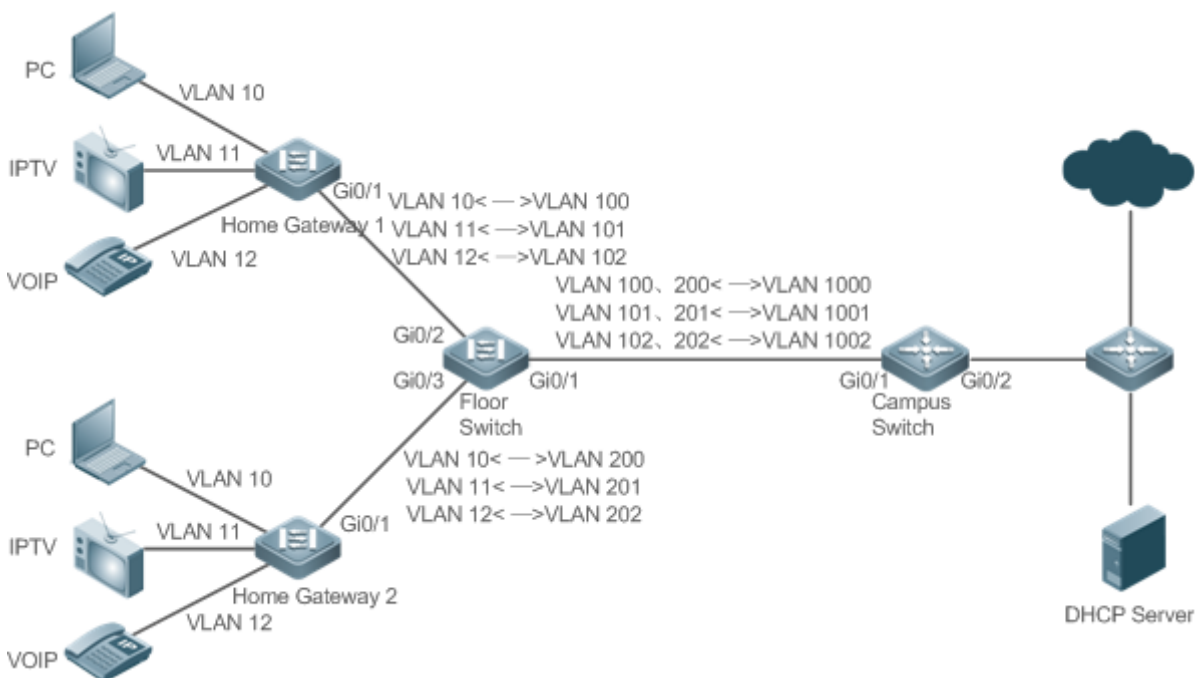
9.2.1 Implementing VLAN Aggregation for Different Services Through VLAN Mapping

Scenario

The different service flows of different users are segregated on a campus network.

- The different service flows are transmitted through different VLANs on the home gateway.
- The same service flows from different users are segregated on the floor switch.
- The same service flows from different users are sent by a campus switch through one single VLAN.

Figure 9-1



Remarks	<p>PC, IPTV, and VoIP are different user services.</p> <p>Switch A and Switch B are the gateway devices of different users.</p> <p>Switch C is a floor switch.</p> <p>Switch D is a campus switch.</p>
----------------	--

Deployment

- On the home gateway devices, configure VLANs for different services to segregate service flows. For example, configure VLAN 10 for the PC service, VLAN 11 for IPTV, and VLAN 12 for VoIP.
- On the ports of the floor switch (Switch D) connected to the home gateway devices, configure VLAN mapping to segregate the service flows of different users.
- On the campus switch, configure VLAN mapping to segregate the service flows.
- Through the preceding deployment, the different service flows of different users are segregated.

9.3 Features

Overview

Feature	Description
VLAN Mapping	Replaces the customer tags of packets with service provider tags, and then restores the service provider tags to customer tags based on the same rules.

9.3.1 VLAN Mapping

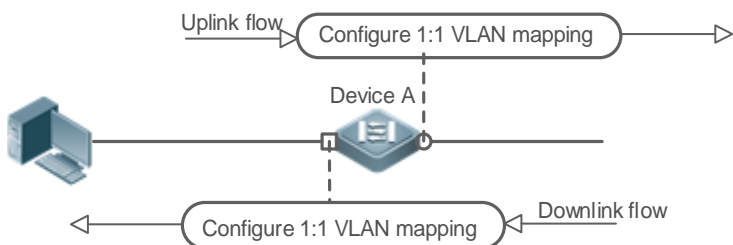
Working Principle

The customer tag of a packet is replaced by a service provider tag to allow the packet to be transmitted based on the public network topology. When the packet is transmitted to the customer network, the service provider tag is restored to

the original customer tag based on the same rule. This device supports 1:1 VLAN mapping rule in the outbound direction.


1:1 VLAN mapping is mainly applied on floor switches to use different VLANs to carry the same services from different users, as shown in Figure 9-2.

Figure 9-2



- Configure the Uplink port with a VLAN mapping policy in the outbound direction to map the customer tag of the uplink flow to the service provider tag.
- Configure the Downlink port with a VLAN mapping policy in the outbound direction to map the service provider tag of the downlink flow to the original customer tag.

9.4 Configuration

Configuration	Description and Command
Configuring VLAN Mapping	 (Mandatory) It is used to enable VLAN mapping.
	vlan-mapping-out vlan <i>svlan</i> remark <i>cvlan</i>


9.4.1 Configuring VLAN Mapping


Configuration Effect

- Replace the customer tags of the packets with the service provider tags to allow the packets to be transmitted based on the VLAN planning on the SP network.

Notes

- VLAN mapping can be configured only on Access ports, Trunk ports, Hybrid ports, or Uplink ports.
- VLAN mapping does not take effect on untagged packets.

 After VLAN mapping is configured, the VLAN IDs of the packets sent to the CPU are changed to the specified VLAN ID.

 It is not recommended to configure VLAN mapping and selective QinQ on the same port.

Configuration Steps

➤ **Configuring 1:1 VLAN Mapping**

- Mandatory if the 1:1 mode is used. Configure a 1:1 VLAN mapping rule.
- Run the **vlan-mapping-out vlan src-vlan remark dest-vlan** command on a Trunk port or an Uplink port to enable 1:1 VLAN mapping.

Command	vlan-mapping-out vlan src-vlan remark dest-vlan
Parameter	src-vlan: Indicates the source VLAN.
Description	dest-vlan: Indicates the destination VLAN.
Defaults	There are no rules
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure 1:1 VLAN mapping in the outbound direction.

- Run the **show interfaces[interface-type interface-number] vlan-mapping** command to display the VLAN mapping configuration.

Configuration

Example

➤ **Implementing VLAN Aggregation for Different Services Through VLAN Mapping**

<p>Scenario Figure 9-3</p>	<p>The diagram illustrates a network topology for implementing VLAN aggregation. It features two Home Gateways (Home Gateway1 and Home Gateway2), a Floor Switch, and a Campus Switch. Home Gateway1 is connected to a PC (VLAN 10), IPTV (VLAN 11), and VoIP (VLAN 12) via its Gi0/2, Gi0/3, and Gi0/4 ports. Home Gateway2 is similarly connected to a PC (VLAN 10), IPTV (VLAN 11), and VoIP (VLAN 12) via its Gi0/2, Gi0/3, and Gi0/4 ports. The Floor Switch is connected to Home Gateway1 (Gi0/1), Home Gateway2 (Gi0/1), and the Campus Switch (Gi0/1). The Campus Switch is connected to the Internet (VLAN 1000), IPTV (VLAN 1001), and VoIP (VLAN 1002) via its Gi0/2 port. Mapping rules are shown in dashed boxes: Home Gateway1 maps VLAN 10 to 100, VLAN 11 to 101, and VLAN 12 to 102; Home Gateway2 maps VLAN 10 to 200, VLAN 11 to 201, and VLAN 12 to 202; the Floor Switch maps VLAN 10 to 100, VLAN 11 to 101, and VLAN 12 to 102; and the Campus Switch maps VLAN 100 to 1000, VLAN 101 to 1001, and VLAN 102 to 1002.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure Home Gateway 1. <p>Step 1: Configure the original VLANs and mapped VLANs for different services.</p> <pre>HGW1> enable HGW1# configure terminal HGW1(config)# vlan range 10-12,100-102 HGW1(config-vlan-range)# exit</pre> <p>Step 2: Configure an Uplink port, then configure 1:1 VLAN mapping policies in the outbound direction.</p>

```
HGW1(config)# interface gigabitethernet 0/1
HGW1(config-if-GigabitEthernet 0/1)# switchport mode uplink
HGW1(config-if-GigabitEthernet 0/1)# vlan-mapping-out vlan 10 remark 100
HGW1(config-if-GigabitEthernet 0/1)# vlan-mapping-out vlan 11 remark 101
HGW1(config-if-GigabitEthernet 0/1)# vlan-mapping-out vlan 12 remark 102
HGW1(config-if-GigabitEthernet 0/1)# exit
```

Step 3: Configure the attributes of the ports connected to PC, IPTV, and VoIP. Assume that the connected ports are Gi 0/2, Gi 0/3, and Gi 0/4 respectively.

```
HGW1(config)#interface gigabitEthernet 0/2
HGW1(config-if-GigabitEthernet 0/2)#switchport mode access
HGW1(config-if-GigabitEthernet 0/2)#switchport access vlan 10
HGW1(config-if-GigabitEthernet 0/2)#exit
HGW1(config)#interface gigabitEthernet 0/3
HGW1(config-if-GigabitEthernet 0/3)#switchport mode access
HGW1(config-if-GigabitEthernet 0/3)#switchport access vlan 11
HGW1(config-if-GigabitEthernet 0/3)#exit
HGW1(config)#interface gigabitEthernet 0/4
HGW1(config-if-GigabitEthernet 0/4)#switchport mode access
HGW1(config-if-GigabitEthernet 0/4)#switchport access vlan 12
HGW1(config-if-GigabitEthernet 0/4)#exit
```

- **Configure Home Gateway 2.**

Step 1: Configure the original VLANs and mapped VLANs for different services.

```
HGW2> enable
HGW2# configure terminal
HGW2(config)# vlan range 10-12,200-202
HGW2(config-vlan-range)# exit
```

Step 2: Configure an Uplink port, then configure 1:1 VLAN mapping policies in the outbound direction.

```
HGW2(config)# interface gigabitethernet 0/1
HGW2(config-if-GigabitEthernet 0/1)# switchport mode uplink
HGW2(config-if-GigabitEthernet 0/1)# vlan-mapping-out vlan 10 remark 200
HGW2(config-if-GigabitEthernet 0/1)# vlan-mapping-out vlan 11 remark 201
HGW2(config-if-GigabitEthernet 0/1)# vlan-mapping-out vlan 12 remark 202
```

Step 3: Configure the attributes of the ports connected to PC, IPTV, and VoIP. Assume that the connected ports are Gi 0/2, Gi 0/3, and Gi 0/4 respectively.

```
HGW2(config)# interface range gigabitethernet 0/2-4
HGW2(config-if-range)# switchport mode access
HGW2(config-if-range)# exit
HGW2(config)# interface gigabitethernet 0/2
HGW2(config-if-GigabitEthernet 0/2)# switchport access vlan 10
HGW2(config-if-GigabitEthernet 0/2)# exit
HGW2(config)# interface gigabitethernet 0/3
HGW2(config-if-GigabitEthernet 0/3)# switchport access vlan 11
HGW2(config-if-GigabitEthernet 0/3)# exit
```

```
HGW2(config)# interface gigabitEthernet 0/4
HGW2(config-if-GigabitEthernet 0/4)# switchport access vlan 12
```

- Configure the XS-S1930J switch to act as a floor switch with 1:1 VLAN mapping policies.

Step 1: Configure the original VLANs and mapped VLANs for different services.

```
Floor>enable
Floor#configure terminal
Floor(config)#vlan range 10-12,100-102,200-202
Floor(config-vlan-range)#exit
```

Step 2: On the Downlink port of Home Gateway 1, configure 1:1 VLAN mapping policies in the outbound direction.

```
Floor(config)#interface gigabitEthernet 0/2
Floor(config-if-GigabitEthernet 0/2)#switchport mode uplink
Floor(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 100 remark 10
Floor(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 101 remark 11
Floor(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 102 remark 12
```


Step 3: On the Downlink port of Home Gateway 2, configure 1:1 VLAN mapping policies in the outbound direction.

```
Floor(config)#interface gigabitEthernet 0/3
Floor(config-if-GigabitEthernet 0/3)#switchport mode uplink
Floor(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 200 remark 10
Floor(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 201 remark 11
Floor(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 202 remark 12
```

Step 4: Configure an Uplink port.

```
Floor(config)# interface gigabitEthernet 0/1
Floor(config-if-GigabitEthernet 0/1)#switchport mode uplink
```

- Configure a campus switch with QinQ policies based on customer tags.

 The XS-S1930J switch cannot act as a campus switch as it does not support QinQ policies based on customer tags. The configuration steps are omitted in this manual. Please refer to the configuration guide of campus switch for configuration steps.

Verification

- Display the 1:1 VLAN mapping policies configured on Home Gateway 1.

```
HGW1# show interfaces vlan-mapping
```

Ports	type	Status	Destination-Vlan	Source-Vlan-list
Gi0/1	out	active	100	10
Gi0/1	out	active	101	11
Gi0/1	out	active	102	12

- Display the 1:1 VLAN mapping policies configured on Home Gateway 2.

```
HGW2# show interfaces vlan-mapping
```

Ports	type	Status	Destination-Vlan	Source-Vlan-list
Gi0/1	out	active	200	10
Gi0/1	out	active	201	11

	Gi0/1	out	active	202	12
	<ul style="list-style-type: none"> ● Display the 1:1 VLAN mapping policies configured on the floor switch. 				
	Floor#show interfaces vlan-mapping				
	Ports	type	Status	Destination-Vlan	Source-Vlan-list
	-----	-----	-----	-----	-----
	Gi0/2	out	active	10	100
	Gi0/2	out	active	11	101
	Gi0/2	out	active	12	102
	Gi0/3	out	active	10	200
	Gi0/3	out	active	11	101
	Gi0/3	out	active	12	202

9.5 Monitoring

Displaying

Description	Command
Displays VLAN mapping on ports.	show interfaces [<i>interface-type interface-number</i>] vlan-mapping

10 Configuring STP/RSTP/MSTP

10.1 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.

Ruijie 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

10.2 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 a 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 PortStates**

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 = RootPort D = Designated Port A = AlternatePort B = BackupPort

Unless otherwise specified, port priorities decrease from left to right.

Figure 10-1

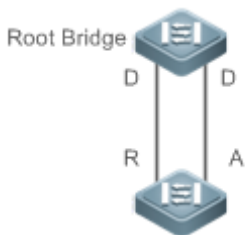


Figure 10-2

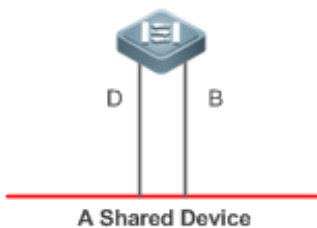
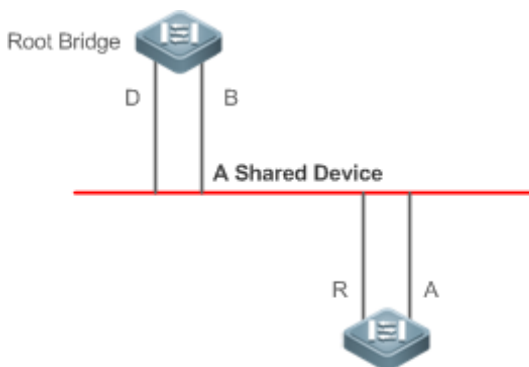


Figure 10-3



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.

10.2.1 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.


Related Configuration

↳ Enabling Spanning-tree

The spanning-tree function is disabled by default.

Run the **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*] command to enable STP. The parameters can configure the basic settings globally.

Forward-time ranges from 4 to 30, hello-time ranges from 1 to 10, and 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: $2 \times (\text{Hello Time} + 1 \text{ second}) \leq \text{Max-Age Time} \leq 2 \times (\text{Forward-Delay Time} - 1 \text{ second})$. Otherwise, the configuration will fail.

10.2.2 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

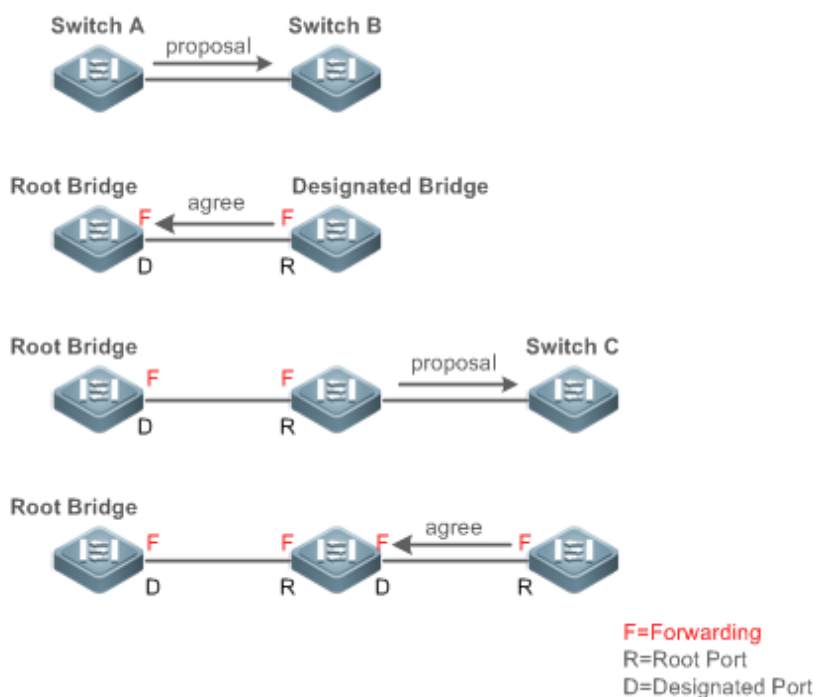
Fast RSTP Convergence

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 10-4, 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 10-4



- i** 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 10-5 and Figure 10-6 show the examples of non point-to-point connection.

Example of non point-to-point connection:

Figure 10-5

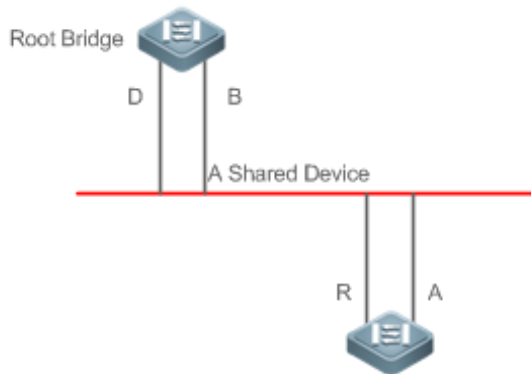


Figure 10-6

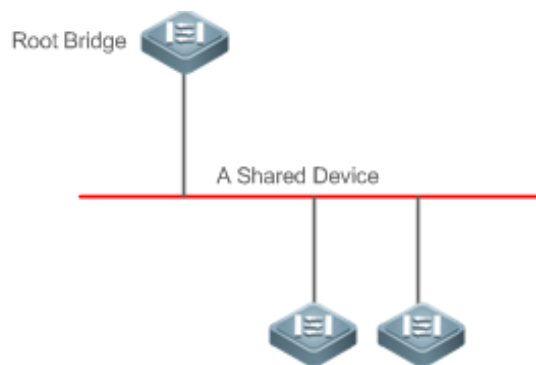
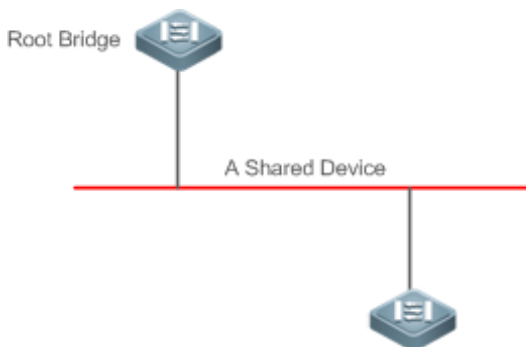


Figure 10-7 shows an example of point-to-point connection.

Figure 10-7



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 the following figures.

Figure 10-8



Figure 10-9



Related Configuration

Configuring Protocol Migration

Run the **clear spanning-tree detected-protocols [interface *interface-id*]** command to enforce version check on the interface. Refer to *Compatibility between RSTP and STP* for more information.

10.2.3 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.

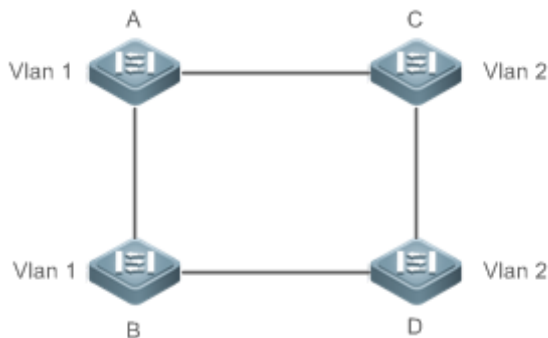
Working Principle

Ruijie 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:

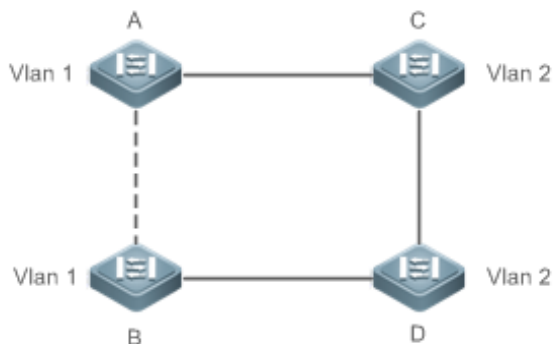
As shown in Figure 10-10, Devices A and B are in VLAN 1 while Devices C and D are in VLAN 2, forming a loop.

Figure 10-10



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 10-11). 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.

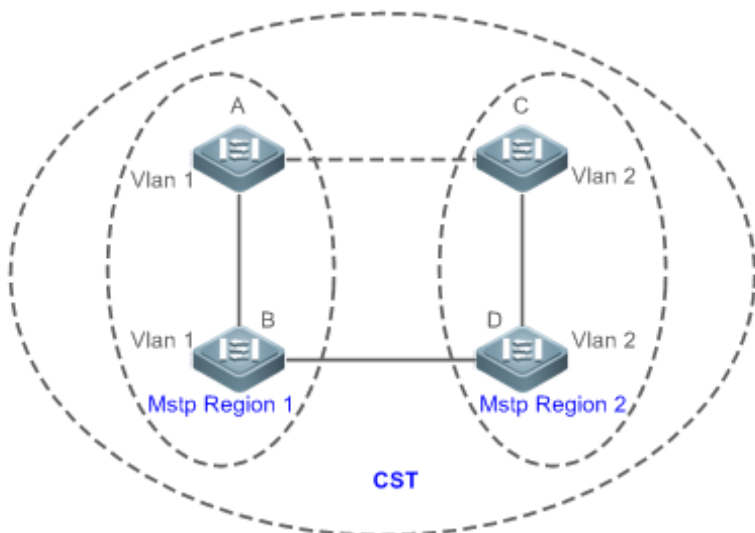
Figure 10-11



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 10-12 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 10-12



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 63 instances (with their IDs ranging from 1 to 63) 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 4,094 VLANs belonging to different instances (ranging from 0 to 63) 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.

i 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)**

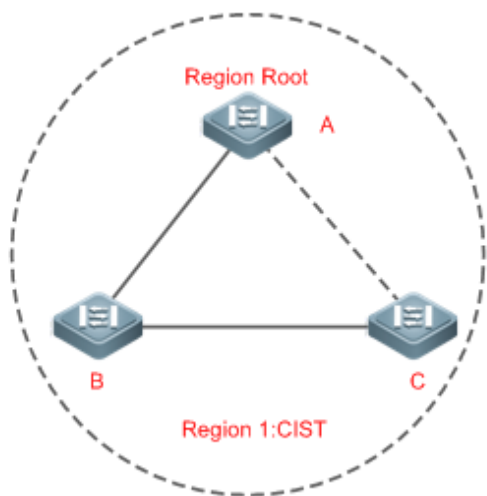
After MSTP regions are divided, each region selects an independent root bridge for each instance based on the corresponding parameters such as bridge priority and port priority, assigns roles to each port on each device, and specifies whether the port is in forwarding or discarding state in the instance based on the port role.

Through MSTP BPDUs 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 10-13, Devices A, B, and C form a loop in Region 1.

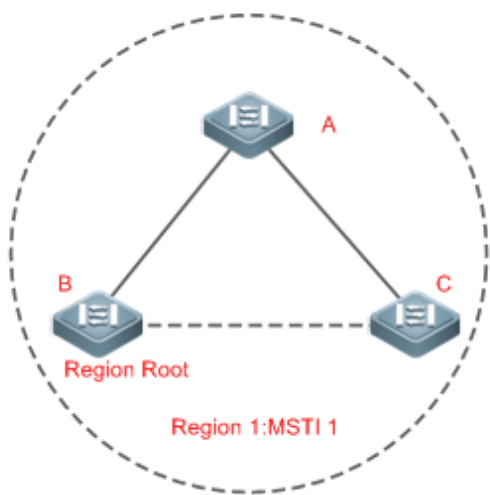
As shown in Figure 10-13, Device A has the highest priority in the CIST (Instance 0) and thereby is selected as the region root. Then MSTP enables the link between A and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 0, only links from A to B and from B to C are available, interrupting the loop of this VLAN group.

Figure 10-13



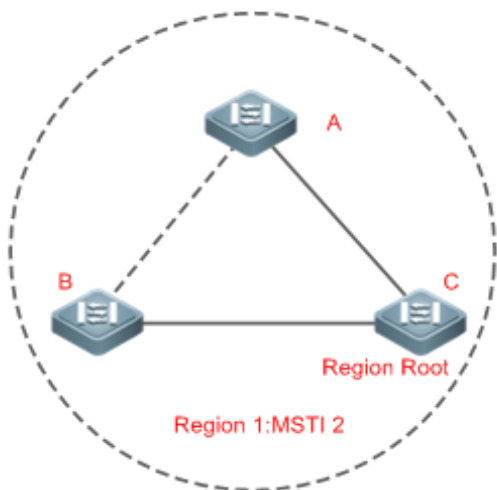
As shown in Figure 10-14, Device B has the highest priority in the MSTI 1 (Instance 1) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 1, only links from A to B and from A to C are available, interrupting the loop of this VLAN group.

Figure 10-14



As shown in Figure 10-15, 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 10-15

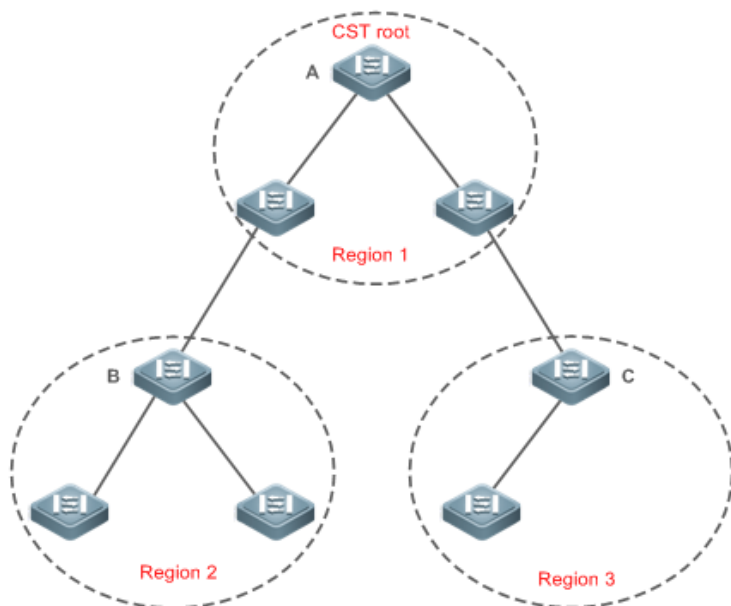


Note that MSTP does not care which VLAN a port belongs to. Therefore, users should configure the path cost and priority of a related port based on the actual VLAN configuration to prevent MSTP from interrupting wrong loops.

📌 **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 10-16, 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 10-16



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.

Related Configuration

Configuring STP mode

STP is set as MSTP by default.

Run the **spanning-tree mode { stp | rstp | mstp }** command to change STP mode.

10.2.4 MSTP Optional Features

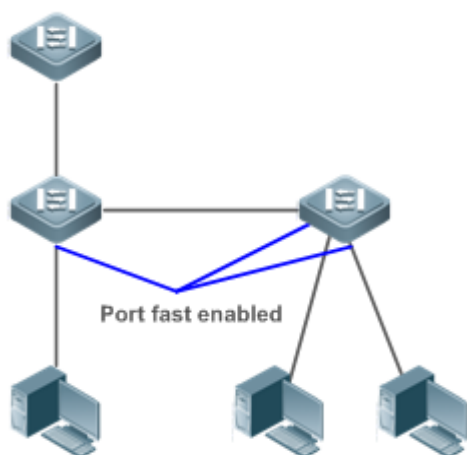
MSTP optional features mainly include PortFast port, BPDU guard, BPDU filter, TC guard, and guard. The optional features are mainly used to deploy MSTP configurations based on the network topology and application characteristics in the MSTP network. This enhances the stability, robustness, and anti-attack 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 10-17 shows which ports of a device can be configured as PortFast ports.

Figure 10-17



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.

Related Configuration

↳ Configuring Portfast on the Interface

PortFast on the interface is disabled by default.

On the global mode, run the **spanning-tree portfast default** command to enable PortFast on all interfaces; run the **no spanning-tree portfast default** command to disable PortFast on all interfaces.

On the interface configuration mode, run the **spanning-tree portfast** command to enable PortFast on an interface; run the **spanning-tree portfastdisabled** command to disable PortFast on an interface.

↳ Configuring BPDU Guard on the Interface

BPDU guard on the interface is disabled by default.

On the global mode, run the **spanning-tree portfast bpduguard default** command to enable BPDU guard on all interfaces; run the **no spanning-tree portfast bpduguard default** command to disable BPDU guard on all interfaces.

On the interface configuration mode, run the **spanning-tree bpduguardenabled** command to enable BPDU guard on an interface; run the **spanning-tree bpduguarddisabled** command to disable BPDU guard on an interface.

↳ Configuring BPDU Filter on the Interface

BPDU Filter on the interface is disabled by default.

On the global mode, run the **spanning-tree portfast bpdufilter default** command to enable BPDU Filter on all interfaces; run the **no spanning-tree portfast bpdufilter default** command to disable BPDU Filter on all interfaces.

On the interface configuration mode, run the **spanning-tree bpdudfilter enabled** command to enable BPDU Filter on an interface; run the **spanning-tree bpdudfilter disabled** command to disable BPDU Filter on an interface.

▾ Configuring Tc-protection on the Interface

Tc-protection is disabled by default.

On the global mode, run the **spanning-tree tc-protection** command to enable Tc-protection on all interfaces; run the **no spanning-tree tc-protection** command to disable Tc-protection on all interfaces.

Tc-protection can only be enabled or disabled globally.

▾ Configuring TC Guard on the Interface

TC Guard on the interface is disabled by default.

On the global mode, run the **spanning-tree tc-protection tc-guard** command to enable tc guard on all interfaces; run the **no spanning-tree tc-protection tc-guard** command to disable tc guard on all interfaces.

On the interface configuration mode, run the **spanning-tree tc-guard** command to enable tc guard on an interface; run the **no spanning-tree tc-guard** command to disable tc guard on an interface.

▾ Configuring TC Filtering on the Interface

TC Filtering on the interface is disabled by default.

On the interface configuration mode, run the **spanning-tree ignore tc** command to enable TC filtering on an interface; run the **no spanning-tree ignore tc** command to disable TC filtering on an interface.

▾ Configuring BPDU Source MAC Check on the Interface

BPDU Source MAC Check on the interface is disabled by default.

On the interface configuration mode, run the **bpdu src-mac-check H.H.H** command to enable BPDU Source MAC Check on an interface; run the **no bpdu src-mac-check** command to disable BPDU Source MAC Check on an interface.

▾ Configuring Auto Edge on the Interface

Auto Edge on the interface is disabled by default.

On the interface configuration mode, run the **spanning-tree autoedge** command to enable Auto Edge on an interface; run the **spanning-tree autoedgedisabled** command to disable Auto Edge on an interface.

▾ Configuring Root Guard on the Interface

Root Guard on the interface is disabled by default.

On the interface configuration mode, run the **spanning-tree guard root** command to enable Root Guard on an interface; run the **no spanning-tree guard root** command to disable Root Guard on an interface.

▾ Configuring Loop Guard on the Interface

Loop Guard on the interface is disabled by default.

On the global mode, run the **spanning-tree loopguard default** command to enable Loop Guard on all interfaces; run the **no spanning-tree loopguard default** command to disable Loop Guard on all interfaces.

On the interface configuration mode, run the **spanning-tree guard loop** command to enable Loop Guard on an interface; run the **no spanning-tree guard loop** command to disable Loop Guard on an interface.

↘ **Configuring BPDU Transparent Transmission on the Interface**







BPDU Transparent Transmission is disabled by default.

On the global mode, run the **bridge-frame forwarding protocol bpdu** command to enable BPDU Transparent Transmission; run the **no bridge-frame forwarding protocol bpdu** command to disable BPDU Transparent Transmission.

BPDU Transparent Transmission is enabled only when STP protocol is disabled.

10.3 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.

Configuration	Description and Command	
Enabling PortFast-related Features	 (Optional) It is used to enable PortFast-related features.	
	spanning-tree portfast	Enables PortFast on a port.
	spanning-tree portfast default	Enables PortFast on all ports.
	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.
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.
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.
Enabling BPDU Transparent Transmission	 (Optional) It is used to enable BPDU transparent transmission	
	bridge-frame forwarding protocol bpdu	Enables BPDU transparent transmission.

10.3.1 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.

Command	spanning-tree [forward-time <i>seconds</i> hello-time <i>seconds</i> max-age <i>seconds</i> tx-hold-count <i>tx-hold-count</i>]
Parameter Description	<p>forward-time <i>seconds</i>: Indicates the interval when the port status changes. The value ranges from 4 to 30 seconds. The default value is 15 seconds.</p> <p>hello-time <i>seconds</i>: Indicates the interval when a device sends a BPDU packet. The value ranges from 1 to 10 seconds. The default value is 2 seconds.</p> <p>max-age <i>second</i>: Indicates the longest TTL of a BPDU packet. The value ranges from 6 to 40 seconds. The default value is 20 seconds.</p> <p>tx-hold-count <i>tx-hold-count</i>: Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.</p>
Defaults	STP is disabled by default.
Command Mode	Global configuration mode
Usage Guide	<p>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:</p> $2 \times (\text{Hello Time} + 1 \text{ second}) \leq \text{Max-Age Time} \leq 2 \times (\text{Forward-Delay Time} - 1 \text{ second})$ <p>Otherwise, the topology may become unstable and the configuration will fail.</p>

▾ 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, Ruijie provides a command for the administrator to switch the STP mode to a lower version if other vendors' devices are incompatible with Ruijie devices.
- Run the **spanning-tree mode { stp | rstp | mstp }** command to modify the STP mode.


Command	spanning-tree mode { stp rstp mstp }
Parameter Description	<p>stp: Spanning Tree Protocol (IEEE 802.1d).</p> <p>rstp: Rapid Spanning Tree Protocol (IEEE 802.1w).</p> <p>mstp: Multiple Spanning Tree Protocol (IEEE 802.1s).</p>
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 Ruijie 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

<p>Scenario Figure 10-18</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>DEV A</p>	<p>Step 1: Enable STP and set the STP mode to STP.</p> <pre>Ruijie#configure terminal Ruijie(config)#spanning-tree Ruijie(config)#spanning-tree mode stp</pre> <p>Step 2: Configure the timer parameters of root bridge DEV A.</p> <pre>Ruijie(config)#spanning-tree hello-time 4 Ruijie(config)#spanning-tree max-age 25 Ruijie(config)#spanning-tree forward-time 18</pre>
<p>DEV B</p>	<p>Enable STP and set the STP mode to STP.</p> <pre>Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#spanning-tree Ruijie(config)#spanning-tree mode stp</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Run the show spanning-tree summary command to display the spanning tree topology and protocol configuration parameters.
<p>DEV A</p>	<pre>Ruijie#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0 Address 00d0.f822.3344</pre>

	<pre> 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 </pre>
DEV B	<pre> Ruijie#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) </pre>

Common Errors

- The STP timer parameters will take effect only when the device is set as the root bridge of the STP.

10.3.2 Configuring STP Compatibility

Configuration Effect

- Enable the compatibility mode of a port to realize interconnection between Ruijie 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 Ruijie devices and other SPs' devices.

Configuration Steps

↳ Enabling the Compatibility Mode on a Port

- Optional.

Command	spanning-tree compatible enable
Parameter	N/A
Description	
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 Ruijie 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.

Command	clear spanning-tree detected-protocols [interface <i>interface-id</i>]
Parameter	interface <i>interface-id</i> : Indicates a port.
Description	
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

<p>Scenario Figure 10-19</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>DEV A</p>	<p>Step 1: Configure Instances 1 and 2, and map Instances 1 and 2 respectively with VLANs 10 and 20.</p> <pre>Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#spanning-tree mst configuration Ruijie(config-mst)#instance 1 vlan 10 Ruijie(config-mst)#instance 2 vlan 20</pre> <p>Step 2: Configure the VLAN the port belongs to, and enable STP compatibility on the port.</p> <pre>Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#switchport access vlan 10 Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable Ruijie(config-if-GigabitEthernet 0/1)#interface gigabitethernet 0/2 Ruijie(config-if-GigabitEthernet 0/2)#switchport access vlan 20 Ruijie(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable</pre>
<p>DEV B</p>	<p>Perform the same steps as DEV A.</p>
<p>Verification</p>	<ul style="list-style-type: none"> ● Run the show spanning-tree summary command to check whether the spanning tree topology is correctly calculated.
<p>DEV A</p>	<pre>Ruijie#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</pre>

```

        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	<pre> Ruijie#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 </pre>						

```

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

10.3.3 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 63, 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 **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	N/A
Description	
Defaults	N/A
Command Mode	Global configuration mode

Usage Guide	Run this command to enter the MST configuration mode.
--------------------	---

Command	instance <i>instance-id</i> vlan <i>vlan-range</i>
Parameter Description	<i>instance-id</i> : Indicates the MSTI ID, ranging from 0 to 63. <i>vlan-range</i> : Indicates the VLAN ID, ranging from 1 to 4,094.
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.

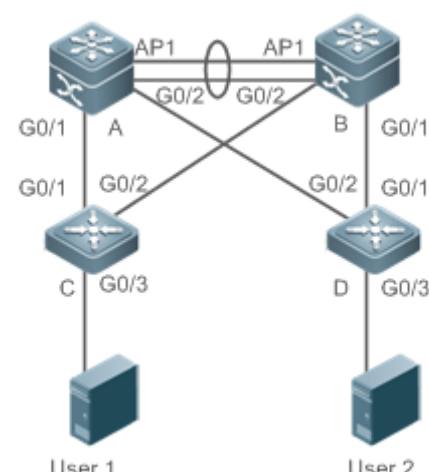
Command	name <i>name</i>
Parameter Description	<i>name</i> : Indicates the MST name. It consists of a maximum of 32 bytes.
Command Mode	MST configuration mode
Usage Guide	N/A

Command	revision <i>version</i>
Parameter Description	<i>version</i> : Indicates the MST revision number, ranging from 0 to 65,535.
Command Mode	MST configuration mode
Usage Guide	N/A

Configuration

Example

↳ Enabling MSTP to Achieve VLAN Load Balancing in the MSTP+VRRP Topology

<p>Scenario Figure 10-20</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>A</p>	<p>Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.</p> <pre>A(config)#vlan 10 A(config-vlan)#vlan 20 A(config-vlan)#exit A(config)#interface range gigabitethernet 0/1 - 2 A(config-if-range)#switchport mode trunk A(config-if-range)#interface aggregateport 1 A(config-if-AggregatePort 1)# switchport mode trunk</pre> <p>Step 2: Enable MSTP and create Instances 1 and 2.</p> <pre>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</pre> <p>Step 3: Configure Switch A as the root bridge of Instances 0 and 1.</p> <pre>A(config)#spanning-tree mst 0 priority 4096 A(config)#spanning-tree mst 1 priority 4096</pre>

	<pre>A(config)#spanning-tree mst 2 priority 8192</pre> <p>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.</p> <pre>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</pre> <p>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.</p> <pre>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</pre>
B	<p>Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.</p> <pre>B(config)#vlan 10 B(config-vlan)#vlan 20 B(config-vlan)#exit B(config)#interface range gigabitethernet 0/1 - 2 B(config-if-range)#switchport mode trunk B(config-if-range)#interface aggregateport 1 B(config-if-AggregatePort 1)# switchport mode trunk</pre> <p>Step 2: Enable MSTP and create Instances 1 and 2.</p> <pre>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</pre> <p>Step 3: Configure Switch A as the root bridge of Instance 2.</p> <pre>B(config)#spanning-tree mst 0 priority 8192 B(config)#spanning-tree mst 1 priority 8192 B(config)#spanning-tree mst 2 priority 4096</pre>

	<p>Step 4: Configure the virtual gateway IP address of VRRP.</p> <pre>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</pre> <p>Step 5 Set the VRRP priority to 120 to enable Switch B to act as the VRRP backup device of VLAN 20.</p> <pre>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</pre>
C	<p>Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.</p> <pre>C(config)#vlan 10 C(config-vlan)#vlan 20 C(config-vlan)#exit C(config)#interface range gigabitethernet 0/1 - 2 C(config-if-range)#switchport mode trunk</pre> <p>Step 2: Enable MSTP and create Instances 1 and 2.</p> <pre>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</pre> <p>Step 3: Configure the port connecting Device C directly to users as a PortFast port and enable BPDU guard.</p> <pre>C(config)#interface gigabitethernet 0/3 C(config-if-GigabitEthernet 0/3)#spanning-tree portfast C(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable</pre>
D	<p>Perform the same steps as Device C.</p>
Verification	<ul style="list-style-type: none"> ● 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


```

successfully created.

A
Ruijie#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
    
```

	<pre> 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 </pre>
B	<pre> Ruijie#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 </pre>

	<pre> 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 </pre>
<p>C</p>	<pre> Ruijie#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 </pre>

```

Bridge ID Priority    32768
      Address    001a. a979. 00ea
      Hello Time  2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface      Role Sts Cost      Prio   Type  OperEdge
-----
Gi0/2          Altn BLK 200000   128    P2p   False
Gi0/1          Root FWD 200000   128    P2p   False

MST 1 vlans map : 10
  Region Root Priority  4096
      Address    00d0. f822. 3344
      this bridge is region root

  Bridge ID Priority    32768
      Address    001a. a979. 00ea

Interface      Role Sts Cost      Prio   Type  OperEdge
-----
Gi0/2          Altn BLK 200000   128    P2p   False
Gi0/1          Root FWD 200000   128    P2p   False

MST 2 vlans map : 20
  Region Root Priority  4096
      Address    001a. a917. 78cc
      this bridge is region root

  Bridge ID Priority    32768
      Address    001a. a979. 00ea

Interface      Role Sts Cost      Prio   Type  OperEdge
-----
Gi0/2          Root FWD 200000   128    P2p   False
Gi0/1          Altn BLK 200000   128    P2p   False
    
```

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.

10.3.4 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	point-to-point: Forcibly configures the link type of a port to be point-to-point.
Description	shared: Forcibly configures the link type of a port to be 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.
----------------------------	--

	<pre>Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point</pre>
Verification	<ul style="list-style-type: none"> ● Run the show spanning-tree summary command to display the link type of the port.
	<pre>Ruijie#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</pre>

Common Errors

N/A

10.3.5 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 and 440. They are integral multiples of 4,096. The default value is 32 and 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 and 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 <i>instance-id</i>] priority <i>priority</i>
Parameter	mst <i>instance-id</i> : Indicates the instance ID, ranging from 0 to 63.
Description	priority <i>priority</i> : 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 <i>instance-id</i> is 0 while that of <i>priority</i> 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 <i>instance-id</i>] port-priority <i>priority</i>
Parameter	mst <i>instance-id</i> : Indicates the instance ID, ranging from 0 to 63.
Description	port-priority <i>priority</i> : Indicates the port priority. There are 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240. They are integral multiples of 4,096.
Defaults	The default value of <i>instance-id</i> is 0. The default value of <i>priority</i> 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

- 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 Priority

<p>Scenario Figure 10-21</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> 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.
<p>DEV A</p>	<p>Step 1: Enable STP and configure the bridge priority.</p> <pre>Ruijie (config)#spanning-tree Ruijie (config)#spanning-tree mst 0 priority 0</pre> <p>Step 2: Configure the priority of Gi 0/2.</p> <pre>Ruijie (config)#interface gigabitethernet 0/2 Ruijie (config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16</pre>
<p>DEV B</p>	<pre>Ruijie (config)#spanning-tree</pre>
<p>Verification</p>	<ul style="list-style-type: none"> Run the show spanning-tree summary command to display the topology calculation result of the spanning tree.
<p>DEV A</p>	<pre>Ruijie# Ruijie#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</pre>

	<pre> 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 </pre>
DEV B	<pre> Ruijie#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 </pre>

Common Errors

N/A

10.3.6 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. Ruijie 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 three 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

- Ruijie's 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	<code>spanning-tree [mst instance-id] cost cost</code>
Parameter	<code>mst instance-id</code> : Indicates the instance ID, ranging from 0 to 63.
Description	<code>cost cost</code> : Indicates the path cost, ranging from 1 to 200,000,000.

Defaults	The default value of <i>instance-id</i> 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 <i>cost</i> 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 long standard short }
Parameter Description	long: Uses the path cost specified in 802.1t. long 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 10-22	
Configuratio	<ul style="list-style-type: none"> ● Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree.

n Steps	<ul style="list-style-type: none"> 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	<pre>Ruijie(config)#spanning-tree Ruijie(config)#spanning-tree mst 0 priority 0</pre>
DEV B	<pre>Ruijie(config)#spanning-tree Ruijie(config)#interface gigabitethernet 0/2 Ruijie(config-if-GigabitEthernet 0/2)# spanning-tree cost 1</pre>
Verification	<ul style="list-style-type: none"> Run the show spanning-tree summary command to display the topology calculation result of the spanning tree.
DEV A	<pre>Ruijie# Ruijie#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</pre>
DEV B	<pre>Ruijie#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</pre>

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

10.3.7 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 <i>hop-count</i>
Parameter Description	<i>hop-count</i> : Indicates the number of devices a BPDU passes through before being discarded. It ranges from 1 to 40.
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	<ul style="list-style-type: none"> Set the maximum hop count of a BPDU packet to 25.
	<pre>Ruijie(config)# spanning-tree max-hops 25</pre>
Verification	<ul style="list-style-type: none"> Run the show spanning-tree command to display the configuration.
	<pre>Ruijie# 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</pre>

10.3.8 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
Parameter	N/A
Description	
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.

Command	spanning-tree portfast default
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

▾ **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.

Command	spanning-tree portfast bpduguard default
Parameter Description	N/A
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 Description	N/A
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.

Command	spanning-tree portfast bpdufilter default
Parameter Description	N/A
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

Command Mode	Interface configuration mode
Usage Guide	If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

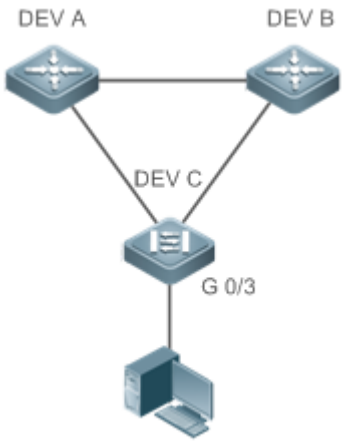
Verification

- 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

Example

Enabling PortFast on a Port

<p>Scenario Figure 10-23</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Configure Gi 0/3 of DEV C as a PortFast port and enable BPDU guard.
<p>DEV C</p>	<pre>Ruijie(config)#interface gigabitethernet 0/3 Ruijie(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. Ruijie(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Run the show spanning-tree interface command to display the port configuration.
<p>DEV C</p>	<pre>Ruijie#show spanning-tree interface gigabitethernet 0/3 PortAdminPortFast : Enabled PortOperPortFast : Enabled</pre>

```
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
```

10.3.9 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.

Command	spanning-tree tc-protection
Parameter	N/A
Description	
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.

Command	spanning-tree tc-protection tc-guard
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	Enable TC guard to prevent TC packets from spreading.

Command	spanning-tree tc-guard
Parameter	N/A
Description	
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.

Command	spanning-tree ignore tc
Parameter	N/A
Description	
Command Mode	Interface configuration mode

Mode	
Usage Guide	If TC filter is enabled on a port, the port does not process received TC packets.

Verification

- Display the configuration.

Configuration

Example

📌 **Enabling TC Guard on a Port**

Configuration Steps	Enable TC guard on a port.
	<pre>Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard</pre>
Verification	<ul style="list-style-type: none"> ● Run the show run interface command to display the TC guard configuration of the port.
	<pre>Ruijie#show run interface gigabitethernet 0/1 Building configuration... Current configuration : 134 bytes interface GigabitEthernet 0/1 switchport mode trunk spanning-tree tc-guard</pre>

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.

10.3.10 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.

Command	bpdu src-mac-check H.H.H
Parameter Description	<i>H.H.H</i> : Indicates an MAC address. The device receives only BPDU packets with this address being the source MAC address.
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.
	<pre>Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 00d0.f800.1234</pre>
Verification	<ul style="list-style-type: none"> ● Run the show run interface command to display the spanning tree configuration of the port.
	<pre>Ruijie#show run interface gigabitethernet 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</pre>

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.

10.3.11 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.

Command	spanning-tree autoedge
Parameter	N/A
Description	
Defaults	Auto Edge is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	<p>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.</p> <p>You can run the spanning-tree autoedge disabled command to disable Auto Edge.</p>

Verification

- Display the configuration.

Configuration

Example

↳ Disabling Auto Edge on a Port

Configuration Steps	<p>Disable Auto Edge on a port.</p> <pre>Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled</pre>
Verification	<ul style="list-style-type: none"> ● Run the show spanning-tree interface command to display the spanning tree configuration of the port. <pre>Ruijie#show spanning-tree interface gigabitethernet 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled</pre>

```
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.

10.3.12 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.

Command	spanning-tree guard root
Parameter	N/A
Description	
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.

Command	spanning-tree loopguard default
Parameter	N/A
Description	
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	N/A
Description	
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

- Display the configuration.

Configuration

Example

▾ Enabling Loop Guard on a Port

<p>Scenario Figure 10-24</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>DEV A</p>	<pre>Ruijie(config)#spanning-tree Ruijie(config)#spanning-tree mst 0 priority 0</pre>
<p>DEV B</p>	<pre>Ruijie(config)#spanning-tree Ruijie(config)# interface range gigabitethernet 0/1-2 Ruijie(config-if-range)#spanning-tree guard loop</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Run the show spanning-tree interface command to display the spanning tree configuration of the port.
<p>DEV A</p>	<pre>Omitted.</pre>
<p>DEV B</p>	<pre>Ruijie#show spanning-tree interface gigabitethernet 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled</pre>

```
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

Ruijie#show spanning-tree interface gigabitethernet 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.

10.3.13 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.

Command	bridge-frame forwarding protocol bpdu
Parameter	N/A
Description	
Defaults	BPDU transparent transmission is disabled by default.
Command Mode	Global configuration mode
Usage	In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved

Guide	<p>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.</p> <p>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.</p>
--------------	--

Verification

- Display the configuration.

Configuration

Example

▾ **Enabling BPDU Transparent Transmission**

Scenario Figure 10-25	
	STP is enabled on DEV A and DEV C while is disabled on DEV B.
Configuration Steps	<ul style="list-style-type: none"> ● Enable BPDU transparent transmission on DEV B so that STP between DEV A and DEV C can be correctly calculated.
DEV B	<pre>Ruijie(config)#bridge-frame forwarding protocol bpdu</pre>
Verification	<ul style="list-style-type: none"> ● Run the show run command to check whether BPDU transparent transmission is enabled.
DEV B	<pre>Ruijie#show run Building configuration... Current configuration : 694 bytes bridge-frame forwarding protocol bpdu</pre>

10.4 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 <i>interface-type interface-number</i>]
Clears the STP topology change information.	clear spanning-tree mst <i>instance-id</i> 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
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 <i>instance-id</i>
Displays MSTP information of the instance corresponding to a port.	show spanning-tree mst <i>instance-id</i> interface <i>interface-id</i>
Displays topology changes of a port in an instance.	show spanning-tree mst <i>instance-id</i> topochange record
Displays MSTP information of all instances corresponding to a port.	show spanning-tree interface <i>interface-id</i>
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

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 bridetect
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

11 Configuring LLDP

11.1 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.

A Ruijie LLDP-compliant device is capable of discovering neighbors when the peer is either of the following:

- Ruijie 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

11.2 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.

11.2.1 Displaying Topology

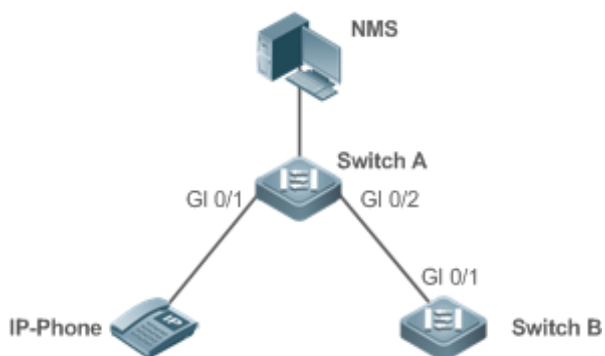
Scenario

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 11-1



Remark	Ruijie Switch A, Switch B, and IP-Phone support LLDP and LLDP-MED.
s	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.

11.2.2 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 11-2



Remark	Ruijie Switch A and Switch B support LLDP.
s	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.

11.3 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 11-3 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 11-4 Ethernet II Format

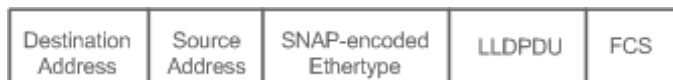


In the preceding figure:

- 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 11-5 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:

1. 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.

- 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

- ✔ Ruijie LLDP-compliant switches support advertisement of basic management TLVs.

- 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.

✔ Ruijie 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.

✔ Ruijie 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.
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.

✔ Ruijie LLDP-compliant Ruijie 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.

11.3.1 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.

11.3.2 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.

11.3.3 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.

11.4 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.
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	Cancel 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	Cancel 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.

Configuration	Description and Command	
	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 <i>value</i>	Configures the TTL multiplier.
	no lldp hold-multiplier	Restores the default TTL multiplier.
	lldp timer tx-interval <i>seconds</i>	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 <i>seconds</i>	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 <i>seconds</i>	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.
	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 <i>profile-num</i>	Configures an LLDP Network Policy.
	no lldp network-policy profile <i>profile-num</i>	Deletes an LLDP Network Policy.
Configuring the Civic	 (Optional) It is used to configure the civic address of a device.	

Configuration	Description and Command	
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 }	Configures the civic address of a device.
	<i>ca-word</i>	
	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 }	Deletes civic address of a device.
	<i>ca-word</i>	
Configuring the Emergency Telephone Number	 (Optional) It is used to configure the emergency telephone number of a device.	
	lldp location elin identifier id <i>elin-location tel-number</i>	Configures the emergency telephone number of a device.
	no lldp location elin identifier id	Deletes the emergency telephone number of a device.

11.4.1 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	N/A
Description	
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	N/A
Description	
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.
	<pre>Ruijie(config)# no lldp enable</pre>
Verification	Display global LLDP status.
	<pre>Ruijie(config)# show lldp status Global status of LLDP: Disable</pre>

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.

11.4.2 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	<code>lldp mode { rx tx txrx }</code>
Parameter	<code>rx</code> : Only receives LLDPDUs.
Description	<code>tx</code> : Only transmits LLDPDUs. <code>txrx</code> : 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	<code>no lldp mode</code>
Parameter	N/A
Description	
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.
	<pre>Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp mode tx</pre>
Verification	Display LLDP status information on the interface.
	<pre>Ruijie(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</pre>

11.4.3 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 <i>tlv-type subtype</i>
Parameter	Parameter <i>tlv-type</i> includes basic-tlv , dot1-tlv , dot3-tlv and med-tlv .
Description	<p>The <i>subtype</i> parameter depends on the <i>tlv-type</i>.</p> <p>basic-tlv: Indicates the basic management TLV.</p> <ul style="list-style-type: none"> ● all : All basic TLVs. ● 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. <p>dot1-tlv: Indicates the IEEE 802.1 organizationally specific TLVs.</p> <ul style="list-style-type: none"> ● all : All dot1 TLVs. ● port-vlan-id: Indicates the Port VLAN ID TLV. ● protocol-vlan-id: Indicates the Port And Protocol VLAN ID TLV. ● <i>vlan-id</i>: Indicates the Port Protocol VLAN ID, ranging from 1 to 4,094. ● vlan-name: Indicates the VLAN Name TLV. ● <i>vlan-id</i>: Indicates the VLAN name, ranging from 1 to 4,094. <p>dot3-tlv: Indicates the IEEE 802.3 organizationally specific TLVs.</p> <ul style="list-style-type: none"> ● all : All dot3 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. <p>med-tlv: Indicates the LLDP MED TLV.</p> <ul style="list-style-type: none"> ● all : All MED TLVs. ● capability: Indicates the LLDP-MED Capabilities TLV. ● inventory: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. ● location { civic-location elin } identifier <i>id</i>: Indicates the Location Identification TLV. <ul style="list-style-type: none"> civic-location: Indicates the civic address information and postal information. elin: Indicates the emergency telephone number. identifier <i>id</i>: Indicates the policy ID, ranging from 1 to 1,024. ● network-policy: Indicates the Network Policy TLV, <i>profile-num</i>: Indicates the Network Policy ID, ranging from 1 to 1,024. ● power-over-ethernet: Indicates the Extended Power-via-MDI TLV.
Command	Interface configuration mode

Mode	
Usage Guide	N/A

↘ **Canceling TLVs**

Command	<code>no lldp tlv-enable tlv-type subtype</code>
Parameter Description	<p>basic-tlv: Indicates the basic management TLV.</p> <ul style="list-style-type: none"> ● all : All basic 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. <p>dot1-tlv: Indicates the IEEE 802.1 organizationally specific TLVs.</p> <ul style="list-style-type: none"> ● all : All dot1 TLV. ● port-vlan-id: Indicates the Port VLAN ID TLV. ● protocol-vlan-id: Indicates the Port And Protocol VLAN ID TLV. ● <i>vlan-id:</i> Indicates the Port Protocol VLAN ID, ranging from 1 to 4,094. ● vlan-name: Indicates the VLAN Name TLV. ● <i>vlan-id:</i> Indicates the VLAN name, ranging from 1 to 4,094. <p>dot3-tlv: Indicates the IEEE 802.3 organizationally specific TLVs.</p> <ul style="list-style-type: none"> ● all : All dot3 TLV. ● 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. <p>med-tlv: Indicates the LLDP MED TLV.</p> <ul style="list-style-type: none"> ● all : All 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 { civic-location elin } identifier id: Indicates the Location Identification TLV. <ul style="list-style-type: none"> ● civic-location: Indicates the civic address information and postal information. ● elin: Indicates the emergency telephone number. ● identifier id: Indicates the policy ID, ranging from 1 to 1,024. ● network-policy: Indicates the Network Policy TLV, <i>profile-num:</i> 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.
	<pre>Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# no lldp tlv-enable dot1-tlv protocol-vlan-id</pre>
Verification	Display LLDP TLV configuration in interface configuration mode.
	<pre>Ruijie(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</pre>

	Inventory TLV	YES	YES
--	---------------	-----	-----

11.4.4 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	<i>ip-address</i> : 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.

▾ 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.

Configuration Example

Configuring the Management Address to Be Advertised

Configuration Steps	Set the management address to 192.168.1.1 on an interface.
	<pre>Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp management-address-tlv 192.168.1.1</pre>
Verification	Display configuration on the interface.
	<pre>Ruijie(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 : 100BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode</pre>

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

11.4.5 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 <i>value</i>
Parameter Description	<i>value</i> : 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.
	<pre>Ruijie(config)# lldp fast-count 5</pre>
Verification	Display the global LLDP status information.
	<pre>Ruijie(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</pre>

11.4.6 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 <i>value</i>
Parameter Description	<i>value</i> : Indicates the TTL 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 <i>seconds</i>
Parameter Description	<i>seconds</i> : 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.
	<pre>Ruijie(config)# lldp hold-multiplier 3 Ruijie(config)# lldp timer tx-interval 20</pre>
Verification	Display the global LLDP status information.
	<pre>Ruijie(config)# lldp hold-multiplier 3 Ruijie(config)# lldp timer tx-interval 20 Ruijie(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</pre>

11.4.7 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 <i>seconds</i>
Parameter Description	<i>seconds</i> : 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.
	<pre>Ruijie(config)# lldp timer tx-delay 3</pre>
Verification	Display the global LLDP status information.
	<pre>Ruijie(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</pre>

11.4.8 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 <i>seconds</i>
Parameter Description	<i>seconds</i> : 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.
	<pre>Ruijie(config)# lldp timer reinit-delay 3</pre>
Verification	Display the global LLDP status information.
	<pre>Ruijie(config)# show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 3s</pre>

Transmit delay	:	2s
Notification interval	:	5s
Fast start counts	:	3

11.4.9 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

Display LLDP 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	N/A
Description	
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	N/A
Description	
Command Mode	Interface configuration mode
Usage	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery

Guide	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 <i>seconds</i>
Parameter Description	<i>seconds</i> : 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.
	<pre>Ruijie(config)# lldp timer notification-interval 10 Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp notification remote-change enable</pre>
Verification	Display LLDP status information.
	<pre>Ruijie(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</pre>

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

11.4.10 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	<code>lldp error-detect</code>
Parameter	N/A
Description	
Command Mode	Interface configuration mode
Usage	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at

Guide	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.
	<pre>Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp error-detect</pre>
Verification	Display LLDP status information on the interface.
	<pre>Ruijie(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</pre>

11.4.11 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	N/A
Description	
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	N/A
Description	
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.
	<pre>Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp encapsulation snap</pre>
Verification	Display LLDP status information on the interface.
	<pre>Ruijie(config-if-GigabitEthernet 0/1)# show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP</pre>

Port encapsulation	: Snap
Operational mode	: RxAndTx
Notification enable	: NO
Error detect enable	: YES
Number of neighbors	: 0
Number of MED neighbors	: 0

11.4.12 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 <i>profile-num</i>
Parameter Description	<i>profile-num</i> : 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	<code>no lldp network-policy profile <i>profile-num</i></code>
Parameter	<i>profile-num</i> : Indicates the LLDP Network Policy ID. The value ranges from 1 to 1,024.
Description	
Command Mode	Interface configuration mode
Usage	Run this command to enter the LLDP network policy mode after specifying a policy ID.
Guide	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.
	<pre>Ruijie#config Ruijie(config)# lldp network-policy profile 1 Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4 Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6 Ruijie(config-lldp-network-policy)# exit Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1</pre>
Verification	Display the LLDP network policy configuration on the local device.
	<pre>network-policy information: ----- network policy profile :1 voice vlan 3 cos 4 voice vlan 3 dscp 6</pre>

11.4.13 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

Display the LLDP civic address of the local device

- Check whether the configuration takes effect.

Related Commands

↘ Entering LLDP Civic Address Configuration Mode

Command	lldp location civic-location identifier <i>id</i>
Parameter Description	<i>id</i> : ID of a common address of a network device, in the range from 1 to 1024.
Command Mode	Global configuration mode
Usage Guide	Use this command to create a common address of a device and enter the LLDP Civic Address configuration mode.

↘ 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 } <i>ca-word</i>
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. <i>ca-word</i> : 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 <i>device-type</i>
Parameter Description	<i>device-type</i> : 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

Configuratio	Set the address of port GigabitEthernet 0/1 as follows: set country to CH, city to Fuzhou, and postal code
---------------------	--

n Steps	to 350000.
	<pre>Ruijie# config Ruijie(config)# lldp location civic-location identifier 1 Ruijie(config-lldp-civic)# country CH Ruijie(config-lldp-civic)# city Fuzhou Ruijie(config-lldp-civic)# postal-code 350000</pre>
Verification	Display the LLDP civic address of port GigabitEthernet 0/1 1.
	<pre>Ruijie# show lldp location civic-location static civic location information: ----- Identifier :1 country :CH device type :1 city :Fuzhou postal-code :350000</pre>

11.4.14 Configuring the Emergency Telephone Number

Configuration Effect

- Configure the emergency telephone number of a device.

Configuration Steps

- Optional.
- Perform this configuration in global configuration mode.

Verification

Display the emergency telephone 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 <i>id</i> elin-location <i>tel-number</i>
Parameter	<i>id</i> : Indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024.
Description	<i>tel-number</i> : Indicates emergency telephone number, containing 10-25 characters.
Command Mode	Global configuration mode
Usage	Run this command to configure the emergency telephone number.

Guide	
--------------	--

📄 [Deleting the Emergency Telephone Number of a Device](#)

Command	<code>no lldp location elin identifier id</code>
Parameter	<i>id</i> : Indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024.
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration

Example

📄 [Configuring the Emergency Telephone Number of a Device](#)

Configuration Steps	Set the emergency telephone number to 085283671111.
	<pre>Ruijie# config Ruijie(config)# lldp location elin identifier 1 elin-location 085283671111</pre>
Verification	Display the emergency telephone number.
	<pre>Ruijie# show lldp location elin-location static elin location information: ----- Identifier :1 elin number :085283671111</pre>

11.5 Monitoring

Clearing

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

Description	Command
Clears LLDP statistics.	<code>clear lldp statistics [interface interface-name]</code>
Clears LLDP neighbor information.	<code>clear lldp table [interface interface-name]</code>

Displaying

Description	Command
Displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.	<code>show lldp local-information [global interface interface-name]</code>

Description	Command
Displays the LLDP civic address or emergency telephone number of a local device.	show lldp location { civic-location elin-location } { identifier <i>id</i> interface <i>interface-name</i> static }
Displays LLDP information on a neighbor.	show lldp neighbors [interface <i>interface-name</i>] [detail]
Displays the LLDP network policy configuration of the local device.	show lldp network-policy { profile [<i>profile-num</i>] interface <i>interface-name</i> }
Displays LLDP statistics.	show lldp statistics [global interface <i>interface-name</i>]
Displays LLDP status information.	show lldp status [interface <i>interface-name</i>]
Displays the configuration of TLVs to be advertised by a port.	show lldp tlv-config [interface <i>interface-name</i>]

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

IP Address & Application Configuration

1. Configuring IP Address and Service
2. Configuring ARP
3. Configuring DHCP
4. Configuring DNS
5. Configuring Network Communication Detection Tools
6. Configuring TCP
7. Configuring IPv4 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

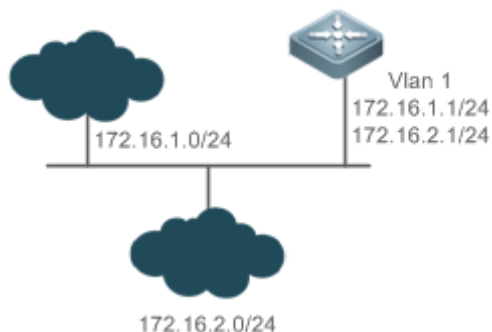
Application	Description
Configuring an IP Address for Communication	Two networks communicate through one switch interface.

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

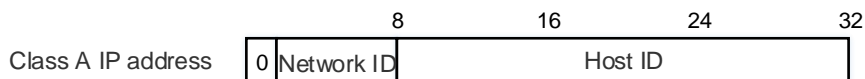
IP Address

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.

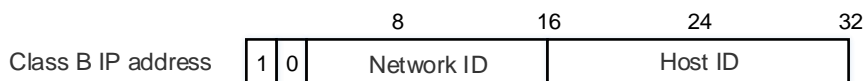
For a class A address, the most significant bit is 0. 7 bits indicate a network ID, and 24 bits indicate a local address. There are 128 class A networks in total.

Figure 1-2



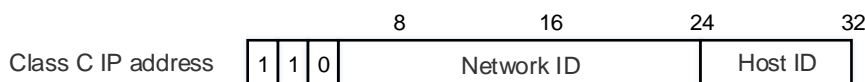
For a class B address, the first two most significant bits are 10. 14 bits indicate a network ID, and 16 bits indicate a local address. There are 16,384 class B networks in total.

Figure 1-3



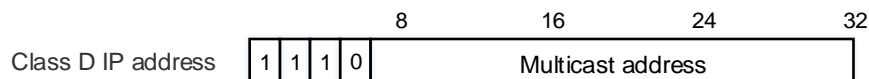
For a class C address, the first three most significant bits are 110. 21 bits indicate a network ID, and 8 bits indicate a local address. There are 2,097,152 class C networks in total.

Figure 1-4



For a class D address, the first four most significant bits are 1110 and other bits indicate a multicast address.

Figure 1-5



i 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. Ruijie 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 TTL	The TTL of unicast packets and broadcast packets is configured.
IP Source Route	Source routes are checked.

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
4. Borrowing IP addresses of other interfaces

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**

Ruijie products support multiple IP address configuration on one interface, of which one is a primary IP address and the others are secondary IP addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, 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.

-
- Before configuring secondary IP addresses, make sure that primary IP addresses are configured. If one device in a network is configured with a secondary IP address, other devices must be configured with secondary IP addresses in the same network. If other devices are not configured with IP addresses, the secondary addresses can be set to primary IP addresses.
-

↳ **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.

↳ **Borrowing an IP Addresses from Another Interface**

One interface may not be configured with an IP address. To enable the interface, it must borrow an IP address from another interface.

-
- IP addresses of Ethernet interfaces, tunnel interfaces, and loopback interfaces can be borrowed. However, these interfaces cannot borrow IP addresses from other interfaces.
-

-  The IP addresses of borrowed interfaces cannot be borrowed from other interfaces.
-  If a borrowed interface has multiple IP addresses, only the primary IP address can be borrowed.
-  The IP address of one interface can be lent to multiple interfaces.
-  IP addresses of borrowing interfaces are always consistent with and vary with IP addresses of borrowed interfaces.

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.

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.

1.3.3 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.

1.3.4 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.

1.3.5 IP Source Route

Working Principle

Ruijie 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.
Configuring the Transmission Rate of ICMP Error Packets	 Optional.
	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 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.

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 <i>ip-address network-mask</i> [secondary]
Parameter	<i>ip-address</i> : 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 (.).
Description	<i>network-mask</i> : 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 SVI 1.
	<pre>Ruijie#configure terminal Ruijie(config)#interface vlan 1 Ruijie(config-if-VLAN 1)# no switchport Ruijie(config-if-VLAN 1)#ip address 192.168.23.110 255.255.255.0</pre>
Verification	Run the show ip interface command to check whether the configuration takes effect.
	<pre>Ruijie# show ip interface VLAN 1 VLAN 1 IP interface state is: UP IP interface type is: BROADCAST IP interface MTU is: 1500 IP address is: 192.168.23.110/24 (primary)</pre>

1.4.2 Configuring Broadcast Address

Configuration Effect

Set the broadcast address of an interface to 0.0.0.0.

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.

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 <i>ip-address</i>
Parameter	<i>ip-address</i> : Broadcast address of an IP network.
Description	
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 RGOS 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.

Configuration Example

Configuration Steps	<p>On interface VLAN 1, set the destination address of IP broadcast packets to 0.0.0.0.</p> <pre>Ruijie#configure terminal Ruijie(config)#interface VLAN 1 Ruijie(config-if-VLAN 1)# no switchport Ruijie(config-if-VLAN 1)#ip broadcast-address 0.0.0.0</pre>
Verification	<p>Run the show ip interface command to check whether the configuration takes effect.</p> <pre>Ruijie#show running-config interface VLAN 1 ip broadcast-address 0.0.0.0</pre>

1.4.3 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 <i>milliseconds</i> [<i>bucket-size</i>]
Parameter Description	<i>milliseconds</i> : 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. <i>bucket-size</i> : 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 10 milliseconds.

📌 **Configuring the Transmission Rate of Other ICMP Error Packets**

Command	<code>ip icmp error-interval milliseconds [bucket-size]</code>
Parameter	<i>milliseconds</i> : Refresh cycle of a token bucket. The value range is 0 to 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.
Description	<i>bucket-size</i> : Number of tokens contained in a token bucket. The value range is 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. 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.
	<pre>Ruijie(config)# ip icmp error-interval DF 1000 100 Ruijie(config)# ip icmp error-interval 1000 10</pre>
Verification	Run the show running-config command to check whether the configuration takes effect.
	<pre>Ruijie#show running-config include ip icmp error-interval ip icmp error-interval 1000 10 ip icmp error-interval DF 1000 100</pre>

1.4.4 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 <i>value</i>
Parameter	<i>value</i> : TTL value. The value range is from 0 to 255.
Description	
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	<ul style="list-style-type: none"> ● Set the TTL of unicast packets to 100. <pre>Ruijie#configure terminal Ruijie(config)#ip ttl 100</pre>
Verification	Run the show run-config command to check whether the configuration takes effect.
	<pre>Ruijie#show running-config ip ttl 100</pre>

1.4.5 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	N/A
Description	
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	<ul style="list-style-type: none"> Disable the IP source route function.
	<pre>Ruijie#configure terminal Ruijie(config)#no ip source-route</pre>
Verification	Run the show run-config command to check whether the configuration takes effect.
	<pre>Ruijie#show running-config no ip source-route</pre>

1.5 Monitoring

Displaying

Description	Command
Displays the IP address of an interface.	show ip interface [<i>interface-type interface-number</i> brief]
Displays IP packet statistics.	show ip packet statistics [total <i>interface-name</i>]
Display IPv4 raw sockets.	show ip raw-socket [<i>num</i>]
Display all IPv4 sockets.	show ip sockets
Display IPv4 UDP sockets.	show ip udp [<i>local-port num</i>]
Display IPv4 UDP socket statistics.	show ip udp statistics

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).

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 Transmission Transparent	With Proxy ARP, a user can directly communicate with users in another network without knowing that it exists.

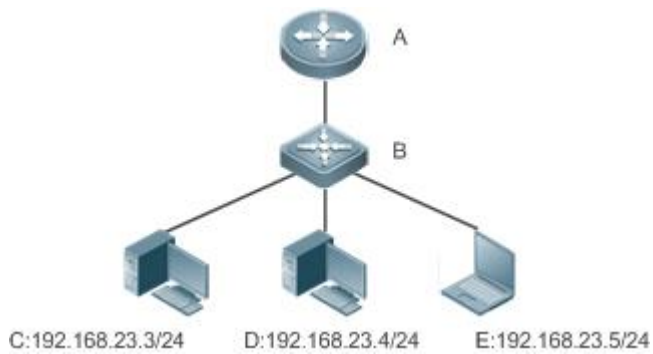
2.2.1 LAN-based ARP

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.

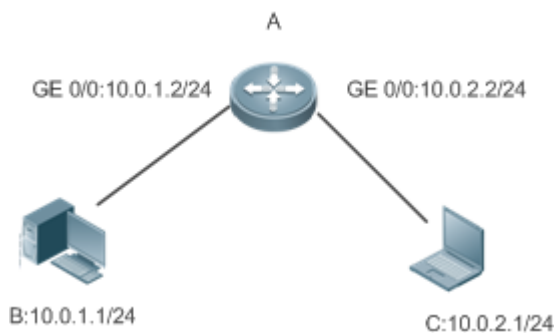
2.2.2 Proxy ARP-based Transparent Transmission

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.
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, and maximum number of ARP entries on an interface.

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 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 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:

1. 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.
2. 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 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.

2.3.5 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	<p> (Optional) It is used to enable static IP-MAC binding.</p> <p>arp Enables static ARP.</p>
Configuring ARP Attributes	<p> (Optional) It is used to specify the ARP timeout, ARP request retransmission interval and times, maximum number of ARP entries on an interface.</p> <p>arp timeout Configures the ARP timeout.</p> <p>arp retry interval Configures the ARP request retransmission interval.</p> <p>arp retry times Configures the ARP request retransmission times.</p> <p>arp cache interface-limit Configures the maximum number of ARP entries on an interface.</p>
Enabling Gratuitous ARP	<p> (Optional) It is used to detect IP address conflicts and enables peripheral devices to update ARP entries.</p> <p>arp gratuitous-send interval Enables gratuitous ARP.</p>
Enabling ARP-based IP Guard	<p> (Optional) It is used to prevent a large number of IP packets from being sent to the CPU.</p> <p>arp anti-ip-attack Configures the number of IP packets for triggering ARP drop.</p>
Enabling ARP Trustworthiness Detection	<p>arp trust-monitor enable Enables egress gateway trusted ARP</p>

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.

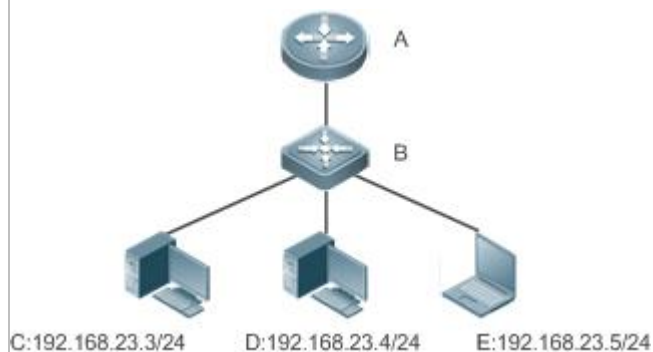
Related Commands

Configuring Static ARP Entries

Command	<code>arp ip-address mac-address type</code>
Parameter	<i>ip-address</i> : Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format.
Description	<i>mac-address</i> : Indicates the DLL address, consisting of 48 bits. <i>type</i> : Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is arpa .
Command Mode	Global configuration mode
Usage Guide	The RGOS 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
Figure 2-3



Remarks	A: Router B: Switch serving as a gateway C, D and E: Users												
Configuration Steps	Configure a static ARP entry on B to statically bind the IP address of A with the MAC address. <pre>Ruijie(config)#arp 192.168.23.1 00D0.F822.334B arpa</pre>												
Verification	Run the show arp static command to display the static ARP entry. <pre>Ruijie(config)#show arp static</pre> <table border="1"> <thead> <tr> <th>Protocol</th> <th>Address</th> <th>Age(min)</th> <th>Hardware</th> <th>Type</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>Internet</td> <td>192.168.23.1</td> <td><static></td> <td>00D0.F822.334B</td> <td>arpa</td> <td></td> </tr> </tbody> </table> <pre>1 static arp entries exist.</pre>	Protocol	Address	Age(min)	Hardware	Type	Interface	Internet	192.168.23.1	<static>	00D0.F822.334B	arpa	
Protocol	Address	Age(min)	Hardware	Type	Interface								
Internet	192.168.23.1	<static>	00D0.F822.334B	arpa									

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, and maximum number of ARP entries on an interface.

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 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, and maximum number of ARP entries on an interface.

Related Commands

↘ Configuring the ARP Timeout

Command	arp timeout <i>seconds</i>
Parameter	<i>seconds</i> : Indicates the timeout in seconds, ranging from 0 to 2,147,483. The default value is 3,600.
Description	
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.

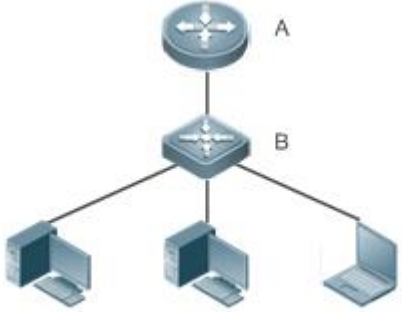
↘ Configuring the ARP Request Retransmission Interval and Times

Command	arp retry interval <i>seconds</i>
Parameter	<i>seconds</i> : Indicates the ARP request retransmission interval in seconds, ranging from 1 to 3,600. The default value is 1.
Description	
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 ARP Entries on an Interface

Command	arp cache interface-limit <i>limit</i>
Parameter	<i>limit</i> : 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 the ARP entry capacity supported by the device. 0 indicates no limit on this number.
Description	
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 Figure 2-4	 <p>C:192.168.23.3/24 D:192.168.23.4/24 E:192.168.23.5/24</p>
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users
Configuration Steps	<ul style="list-style-type: none"> ● Set the ARP timeout to 60 seconds on VLAN 1. ● Set the maximum number of learned ARP entries to 300 on VLAN 1. ● Set the ARP request retransmission interval to 3 seconds. ● Set the ARP request retransmission times to 4.
	<pre>Ruijie(config)#interface VLAN 1 Ruijie(config-if- VLAN 1)#arp timeout 60 Ruijie(config-if- VLAN 1)#arp cache interface-limit 300 Ruijie(config-if- VLAN 1)#exit Ruijie(config)#arp retry interval 3 Ruijie(config)#arp retry times 4</pre>
Verification	<ul style="list-style-type: none"> ● Run the show arp timeout command to display the timeout of the interface. ● Run the show running-config command to display the ARP request retransmission interval and times, and maximum number of ARP entries on the interface.
	<pre>Ruijie#show arp timeout Interface arp timeout(sec) ----- VLAN 1 60 VLAN 100 3600 VLAN 111 3600 Mgmt 0 3600 Ruijie(config)# show running-config arp retry times 4</pre>

```

arp retry interval 3
!
interface VLAN 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]*

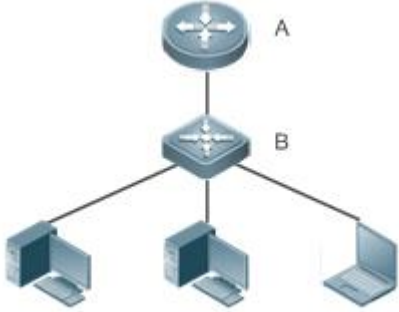
command to check whether the configuration is successful.

Related Commands

↘ Enabling Gratuitous ARP

Command	arp gratuitous-send interval <i>seconds</i> [<i>number</i>]
Parameter Description	<i>seconds</i> : Indicates the interval for sending a gratuitous ARP request. The unit is second. The value ranges from 1 to 3,600. <i>Number</i> : 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 Figure 2-5	 <p>C:192.168.23.3/24 D:192.168.23.4/24 E:192.168.23.5/24</p>
Remarks	A: Router B: Switch serving as a gateway C, D and E: Users
Configuration Steps	Configure the VLAN 1 interface to send a gratuitous ARP packet every 5 seconds.
	<pre>Ruijie(config-if-VLAN 1)#arp gratuitous-send interval 5</pre>
Verification	Run the show running-config interface command to check whether the configuration takes effect.
	<pre>Ruijie#sh running-config interface VLAN 1 Building configuration... Current configuration : 127 bytes ! interface VLAN 1 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp gratuitous-send interval 5</pre>

2.4.4 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	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	<p>❗ Enable this function. If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD.</p> <p>❗ Enable this function. If the MAC address of the existing dynamic ARP entry is updated, the device immediately performs NUD.</p> <p>❗ After this function is disabled, the device does not perform NUD for learning or updating ARP entries.</p>

Configuration Example

Scenario Figure 2-6	<p>C:192.168.23.3/24 D:192.168.23.4/24 E:192.168.23.5/24</p>
Remarks	<p>A: Router</p> <p>B: Switch serving as a gateway</p>

	C, D and E: Users
Configuration Steps	Enable ARP trustworthiness detection on VLAN 1.
	<pre>Ruijie(config-if- VLAN 1)#arp trust-monitor enable</pre>
Verification	Run the show running-config interface command to check whether the configuration takes effect.
	<pre>Ruijie#show running-config interface VLAN 1 Building configuration... Current configuration : 184 bytes ! interface VLAN 1 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp trust-monitor enable</pre>

2.4.5 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

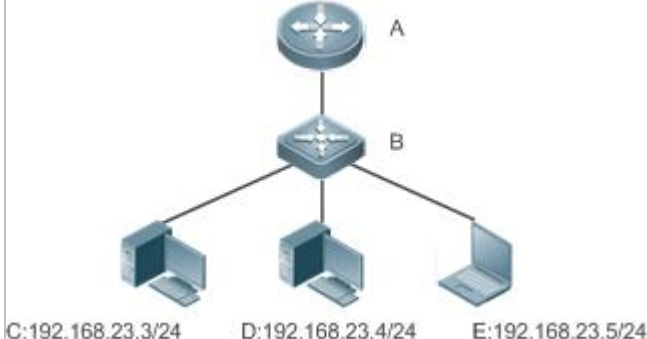
Run the **show run** command to check whether the configuration takes effect.

Related Commands

▾ Enabling ARP-based IP Guard


Command	arp anti-ip-attack num
Parameter	<i>num</i> : Indicates the number of IP packets for triggering ARP drop. The value ranges from 0 to 100.
Description	0 indicates that ARP-based IP guard is disabled. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	<p>❗ 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.</p>

Configuration Example

Scenario Figure 2-7	 <p>C:192.168.23.3/24 D:192.168.23.4/24 E:192.168.23.5/24</p>
Remarks	<p>A: Router</p> <p>B: Switch serving as a gateway</p> <p>C, D and E: Users</p>
Configuration Steps	<p>Enable ARP-based IP guard on B.</p> <pre>Ruijie(config)#arp anti-ip-attack 10</pre>
Verification	<p>Run the show running-config command to check whether the configuration takes effect.</p> <pre>Ruijie#show running-config</pre> <p>Building configuration...</p> <p>Current configuration : 53 bytes</p> <pre>arp anti-ip-attack 10</pre>

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
Clears ARP packet statistics.	clear arp-cache packet statistics [<i>interface</i>]

Displaying

Description	Command
Displays the ARP table in detail.	show arp [detail] [<i>interface-type interface-number</i> [<i>ip</i> [<i>mask</i>] <i>mac-address</i> 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
Displays ARP packet statistics.	show arp packet statistics [<i>interface</i>]

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 DHCP

3.1 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 mode.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions

3.2 Applications

Application	Description
Providing DHCP Service in a LAN	Assigns IP addresses to clients in a LAN.
Enabling DHCP Client	Enable DHCP Client.

3.2.1 Providing DHCP Service in a LAN

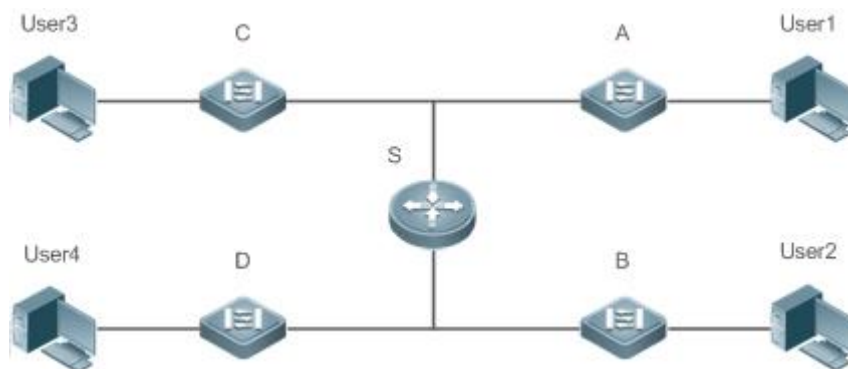
Scenario

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 3-1



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.

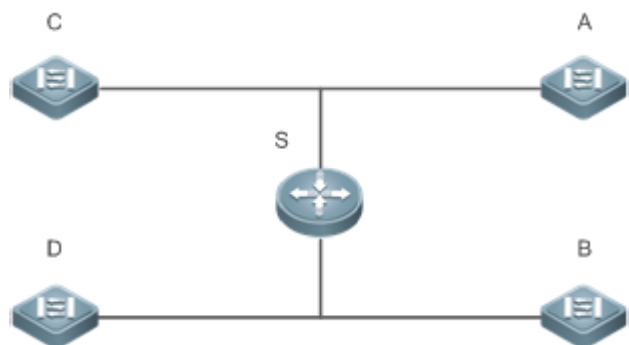
3.2.2 Enabling DHCP Client

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 3-2



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.

3.3 Features

Basic Concepts

↳ DHCP Client

DHCP Client enables a device to automatically obtain an IP address and configurations from a DHCP server.

Overview

Feature	Description
DHCP Client	Enable DHCP Client on a device, and it may obtain IP addresses and configurations automatically from a DHCP server.

3.3.1 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.

3.4 Configuration

▾ 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.

3.4.1 Configuring DHCP Client

Configuration Effect

Enable DHCP Client on a device so that it obtains IP addresses and configurations dynamically.

Notes

Ruijie 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	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	<ul style="list-style-type: none"> ● Ruijie products support dynamic IP address obtainment by an Ethernet interface. ● Ruijie products support dynamic IP address obtainment by a PPP-encapsulated interface. ● Ruijie products support dynamic IP address obtainment by an FR-encapsulated interface. ● Ruijie products support dynamic IP address obtainment by an HDLC-encapsulated interface.

Configuration Example

Configuring DHCP Client

Configuration Steps	1: Enable interface SVI 1 with DHCP to obtain an IP address.
	<pre>Ruijie(config)# interface vlan 1 Ruijie(config-if-VLAN 1)#ip address dhcp</pre>
Verification	1: Run the show run command to display the configuration.
	<pre>Ruijie(config)#show run begin ip address dhcp ip address dhcp</pre>

3.5 Monitoring


Clearing

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

Displaying

Description	Command
Displays DHCP lease.	show dhcp lease

Debugging

 System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs DHCP packets.	debug ip dhcp client

4 Configuring DNS

4.1 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

4.2 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.

4.2.1 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

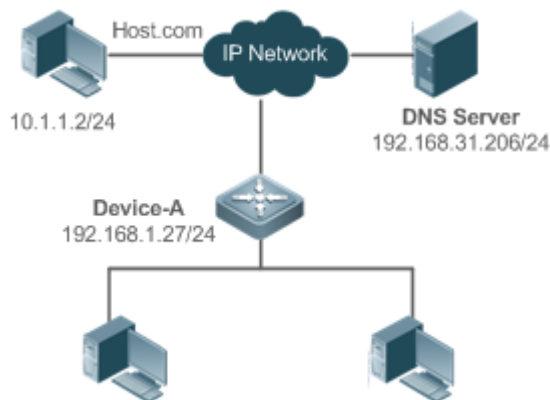
- Preset the mapping between a domain name and an IP address on a device.

4.2.2 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 4-1 Dynamic Domain Name Resolution



Deployment

- Deploy DNS Server as the DNS server of Device-A.

4.3 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.

4.3.1 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:

1. 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.
2. 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.
3. If all domain names expire, the DNS resolver initiates a request for domain name-IP address conversion to the external DNS server.
4. After receiving a response from the DNS server, the DNS resolver caches and transfers the response to the application program.

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.

▾ Configuring a DNS Server

- By default, no DNS server is configured.
- Run the **ip name-server** command to configure a DNS server.

4.4 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.
Configuring Dynamic Domain Name Resolution	 Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip name-server	Configures a DNS server.

4.4.1 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 IPv4 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 <i>host-name ip-address</i>
Parameter	<i>host-name</i> : indicates a domain name.
Description	<i>ip-address</i> : indicates a mapped IPv4 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring Static Domain Name Resolution

Configuration Steps	<ul style="list-style-type: none"> ● Set the IP address of static domain name www.test.com to 192.168.1.1 on a device. <pre>Ruijie#configure terminal Ruijie(config)# ip host www.test.com 192.168.1.1 Ruijie(config)# exit</pre>
Verification	Run the show hosts command to check whether the static domain name entry is configured.
	<pre>Ruijie#show hosts Name servers are: Host type Address TTL(sec)</pre>

	www.test.com	static	192.168.1.1	---
--	--------------	--------	-------------	-----

4.4.2 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 { <i>ip-address</i> }
Parameter	<i>ip-address</i> : indicates the IPv4 address of the DNS server.
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example


▾ Configuring Dynamic Domain Name Resolution

Scenario Figure 4-2	 <p>The diagram shows a network topology. On the left is a 'Device' represented by a blue square with a white cross. A horizontal line connects it to a central cloud icon representing the network. To the right of the cloud is a 'DNS Server' represented by a blue server rack icon, with the IP address '192.168.10.1' written above it.</p>
	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.

	<pre> DEVICE#configure terminal DEVICE(config)# ip name-server 192.168.10.1 DEVICE(config)# exit </pre>
Verification	Run the show hosts command to check whether the DNS server is specified.
	<pre> Ruijie(config)#show hosts Name servers are: 192.168.10.1 static Host type Address TTL(sec) </pre>

4.5 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 [<i>host-name</i>]

Displaying

Description	Command
Displays DNS parameters.	show hosts [<i>host-name</i>]

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

5 Configuring Network Communication Test Tools

5.1 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

5.2 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.

5.2.1 End-to-End Connectivity Test

Scenario

As shown in Figure 5-1, 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 5-1



Deployment

Execute the ping function on the network device.

5.2.2 Host Route Test

Scenario

As shown in Figure 5-2, 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 5-2



Deployment

Execute the traceroute function on the network device.

5.3 Features

Overview

Feature	Description
Ping Test	Test whether the specified IPv4 address is reachable and display the related information.
Traceroute Test	Display the gateways that IPv4 packets pass through when transmitted from the source to the destination.

5.3.1 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.

5.3.2 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.

5.4 Configuration

Configuration	Description and Command
Ping Test	 (Optional) It is used to check whether an IPv4 address is reachable.
	Ping Executes the Ping function.
Traceroute Test	 (Optional) It is used to display the gateways that IPv4 packets pass through when transmitted from the source to the destination.
	Traceroute Executes the traceroute function.

5.4.1 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.

Verification

Run the **ping** command to display related information on the command line interface (CLI) window.

Related Commands

📄 Ping IPv4

Command	<code>ping [ip] [address [length length] [ntimes times] [timeout seconds] [data data] [source source] [df-bit] [validate] [detail] [out-interface interface]]</code>
----------------	--

Parameter Description	<p><i>address</i>: Specifies the destination IPv4 address or domain name.</p> <p><i>length</i>: Specifies the length of the data packet. The value ranges from 36 to 18,024. The default length is 100.</p> <p><i>times</i>: Specifies the number of probes. The value ranges from 1 to 4,294,967,295</p> <p><i>seconds</i>: Specifies the timeout. The value ranges from 1s to 10s.</p> <p><i>data</i>: Specifies the data in the packet. The data is a string of 1 to 255 bytes. By default, the string is "abcd".</p> <p><i>source</i>: 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.</p> <p>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.</p> <p>validate: Configures whether to verify the response packet.</p> <p>detail: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed.</p> <p><i>interface</i>: Specifies the interface for sending the data packets.</p>
Command Mode	<p>In User EXEC mode, you can execute only the basic ping function. In Privileged EXEC mode, you can execute the extended ping function.</p> <p>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.</p>
Configuration Usage	<p>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.</p> <p>To use the domain name, you must first configure the domain name server (DNS). For details about the configuration, see <i>Configuring DNS</i>.</p>

Configuration Example

↳ Executing the Common Ping Function

Configuration Steps	<p>In Privileged EXEC mode, run the ping 192.168.21.26 command.</p>
	<pre> Common ping command: Ruijie# 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: Ruijie#ping 192.168.21.26 detail Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: </pre>

	<pre> < 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. </pre>
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.
	<pre> Common ping command: Ruijie# 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 </pre>

	<pre> 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=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. </pre>
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.

5.4.2 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.

Verification

Run the **traceroute** command to display related information on the CLI window.

Related Commands

Traceroute IPv4

Command	traceroute [ip] [adress [probe number] [source source] [timeout seconds] [ttl minimum maximum]
----------------	---

	[out-interface interface]]
Parameter Description	<p><i>address</i>: Specifies the destination IPv4 address or domain name.</p> <p><i>number</i>: Specifies the number of probes. The value ranges from 1 to 255.</p> <p><i>source</i>: 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.</p> <p><i>seconds</i>: Specifies the timeout. The value ranges from 1s to 10s.</p> <p><i>minimum maximum</i>: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.</p> <p><i>interface</i>: Specifies the interface for sending the data packets.</p>
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 <i>Configuring DNS</i> .

Configuration Example

↘ Executing the Traceroute Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the traceroute ipv6 3004::1 command.
	<pre>Ruijie# traceroute 61.154.22.36 < press Ctrl+C to break > Tracing the route to 61.154.22.36 1 192.168.12.1 0 msec 0 msec 0 msec 2 192.168.9.2 4 msec 4 msec 4 msec 3 192.168.9.1 8 msec 8 msec 4 msec 4 192.168.0.10 4 msec 28 msec 12 msec 5 202.101.143.130 4 msec 16 msec 8 msec 6 202.101.143.154 12 msec 8 msec 24 msec 7 61.154.22.36 12 msec 8 msec 22 msec</pre>
	The preceding test result indicates that the network device accesses host 61.154.22.36 by transmitting packets through gateways 1–6. 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.
	<pre>Ruijie# 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</pre>

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
<p>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.</p>				

6 Configuring TCP

6.1 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 2385: Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022: Management Information Base for the Transmission Control Protocol (TCP)

6.2 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.

6.2.1 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 6-1



REMARKS: A, B, C AND D ARE ROUTERS.

Deployment

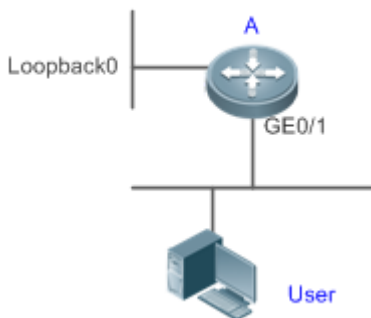
- Enable PMTUD on A and D.

6.2.2 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 6-2



Remarks: A is a router.

Deployment

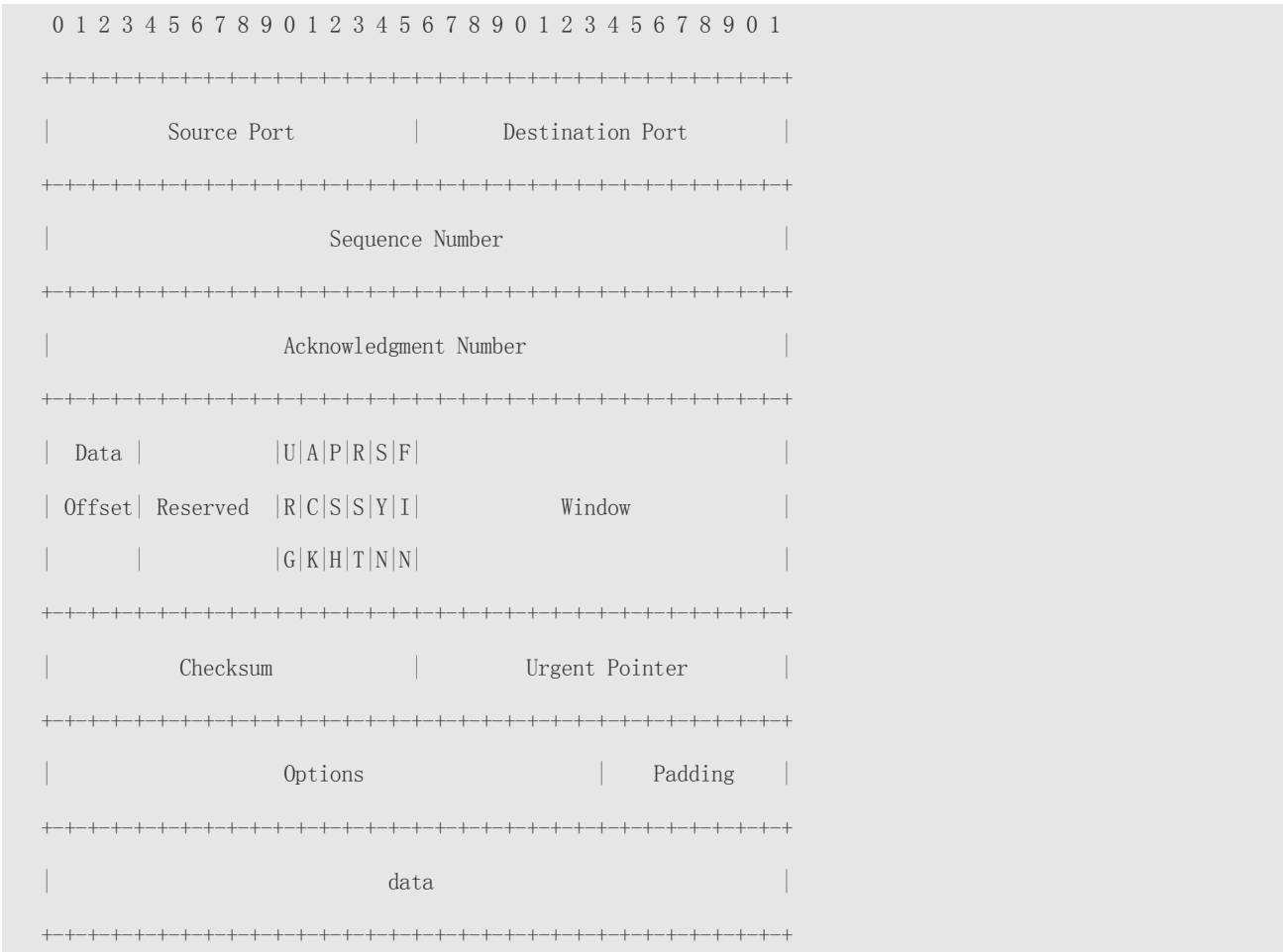
- Enable TCP keepalive on A.

6.3 Features

Basic Concepts

TCP Header Format

0	1	2	3
---	---	---	---



- **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 URG 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:
 1. A client sends a SYN packet to the server.

2. The server receives the SYN packet and responds with a SYN ACK packet.
 3. 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.

6.3.1 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.
- 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.

6.3.2 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.

6.3.3 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.

6.3.4 Configuring MSS

Working Principle

The MSS refers to the total amount of data contained in a TCP segment 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.

- i** The effective MSS is the smaller one between the calculated MSS and the configured MSS.
- i** 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.

6.3.5 Path MTU Discovery

Working Principle

The Path MTU Discovery 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.

6.3.6 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.

 This command applies to both TCP server and client.

6.4 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 Exception	 (Optional) It is used to detect whether the peer works normally.	
	ip tcp keepalive	Enables TCP keepalive.

6.4.1 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 <i>seconds</i>
Parameter	<i>seconds</i> : Indicates SYN packet timeout. It ranges from 5 to 300 seconds. The default is 20 seconds.
Description	
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 <i>size</i>
Parameter	<i>size</i> : Indicates a TCP window size. It ranges from 128 to (65535 << 14) bytes. The default is 65535 bytes.
Description	
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	N/A
Description	
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 <i>max-segment-size</i>
Parameter	<i>max-segment-size</i> : Indicates the maximum segment size. It ranges from 68 to 10000 bytes. By default, the
Description	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 <i>minutes</i> age-timer infinite]
Parameter	age-timer <i>minutes</i> : Indicates the interval for a new probe after a path MTU is discovered. It ranges from 10
Description	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.								
	<pre>Ruijie# configure terminal Ruijie(config)# ip tcp path-mtu-discovery Ruijie(config)# end</pre>								
Verification	Run the show tcp pmtu command to display the IPv4 TCP PMTU.								
	<pre>Ruijie# show tcp pmtu</pre> <table border="1"> <thead> <tr> <th>Number</th> <th>Local Address</th> <th>Foreign Address</th> <th>PMTU</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>192.168.195.212.23</td> <td>192.168.195.112.13560</td> <td>1440</td> </tr> </tbody> </table>	Number	Local Address	Foreign Address	PMTU	1	192.168.195.212.23	192.168.195.112.13560	1440
Number	Local Address	Foreign Address	PMTU						
1	192.168.195.212.23	192.168.195.112.13560	1440						

Common Errors

N/A

6.4.2 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 <i>num1</i>] [times <i>num2</i>] [idle-period <i>num3</i>]
Parameter	interval <i>num1</i> : Indicates the interval to send keepalive packets. Ranging from 1 to120 seconds. The default

Description	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 is 15 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.
	<pre>Ruijie# configure terminal Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180 Ruijie(config)# end</pre>
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

6.5 Monitoring

Displaying

Description	Command
Displays basic information on IPv4 TCP connection.	show tcp connect [local-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-ip <i>a.b.c.d</i>] [peer-port <i>num</i>]
Displays IPv4 TCP connection statistics.	show tcp connect statistics
Displays IPv4 TCP PMTU.	show tcp pmtu [local-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-ip <i>a.b.c.d</i>] [peer-port <i>num</i>]
Displays IPv4 TCP port information.	show tcp port [<i>num</i>]
Displays IPv4 TCP parameters.	show tcp parameter
Displays IPv4 TCP statistics.	show tcp statistics

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.	<code>debug ip tcp packet [in out] [local-ip <i>a.b.c.d</i>] [peer-ip <i>a.b.c.d</i>] [global] [local-port <i>num</i>] [peer-port <i>num</i>] [deeply]</code>
Displays the debugging information on IPv4 TCP connection.	<code>debug ip tcp transactions [local-ip <i>a.b.c.d</i>] [peer-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-port <i>num</i>]</code>

7 Configuring IPv4 REF

7.1 Overview

On products incapable of hardware-based forwarding, IPv4 packets are forwarded through the software. To optimize the software-based forwarding performance, Ruijie introduces IPv4 express forwarding through software (Ruijie Express Forwarding, namely REF).

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 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

7.2 Applications

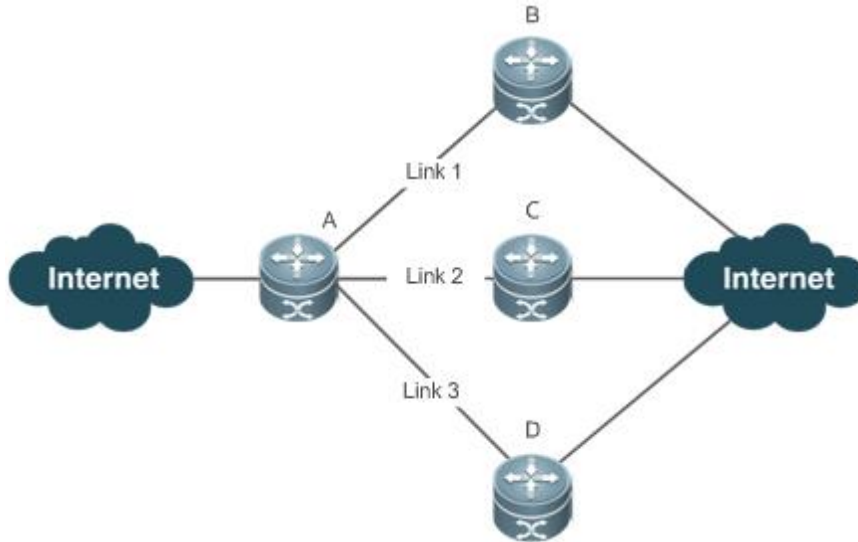
Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among the multiple next hops.

7.2.1 Load Balancing

Scenario

As shown in Figure 7-1, 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 7-1



Remarks	A is a router that runs REF. B, C and D are forwarding devices.
----------------	--

Deployment

- Run REF on router A.

7.3 Features

Basic Concepts

IPv4 REF involves the following basic concepts:

↳ Routing table

An IPv4 routing table stores routes to the specific destinations and contains the topology information. During packet forwarding, IPv4 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.

↘ Packet forwarding path

Packets are forwarded based on their IPv4 addresses. If the source and destination IPv4 addresses of a packet are specified, the forwarding path of this packet is determined.

7.3.1 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 packet is matched with a load balance entry based on the longest prefix match, REF performs hash calculation based on the IPv4 address of the packet and selects a path to forward the packet.

IPv4 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.

7.4 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 REF packet statistics.

Command	Description
show ip ref packet statistics	Displays IPv4 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.

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 .

Displaying Packet Forwarding Path Information

Packets are forwarded based on their IPv4 addresses. If the source and destination IPv4 addresses of a packet are specified, the forwarding path of this packet is determined. Run the following commands and specify the IPv4 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
<code>show ip ref exact-route source-ipaddress dest_ipaddress</code>	Displays the forwarding path of a packet.

Displaying Route Information in an REF Table

Run the following commands to display the route information in an REF table:

Command	Description
<code>show ip ref route [default {ip mask}] statistics]</code>	Displays route information in the IPv4 REF table. The parameter default indicates a default route.

IP Routing Configuration

1. Configuring Managing Routes

1 Managing Routes

1.1 Overview

The network service module (NSM) manages the routing table and selects and sends preferred routes to the routing table. Routes discovered by various routing protocols are stored in the routing table. This product supports the direct route which is discovered by a link-layer protocol and is also called interface route.

1.2 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.

1.2.1 Route Computation

[Routing Function](#)

Routing functions are classified into IPv4 routing functions. If the routing functions are disabled, a device is equivalent to a host and cannot forward routes.

1.2.2 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.



1.2.3 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.

[Default Gateway](#)

On a L2 switch, the **ip default-gateway** command is configured to generate a default route.

1.3 Configuration

Configuration Item	Description and Command	
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.
Configuring Route Limitations	 (Optional) It is used to disable routing.	
	no ip routing	Disables IPv4 routing.

1.3.1 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** command to configure the default gateway.

Configuration Steps

▾ [Configuring the IPv4 Gateway on a L2 Switch](#)

Command	ip default-gateway <i>ip-address</i>	
Parameter	<i>ip-address</i>	Indicates the IPv4 gateway address.
Description		
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

1.3.2 Configuring Route Limitations

Configuration Effect

- Disable routing.

Notes

Route limitations cannot be configured on a L2 switch.

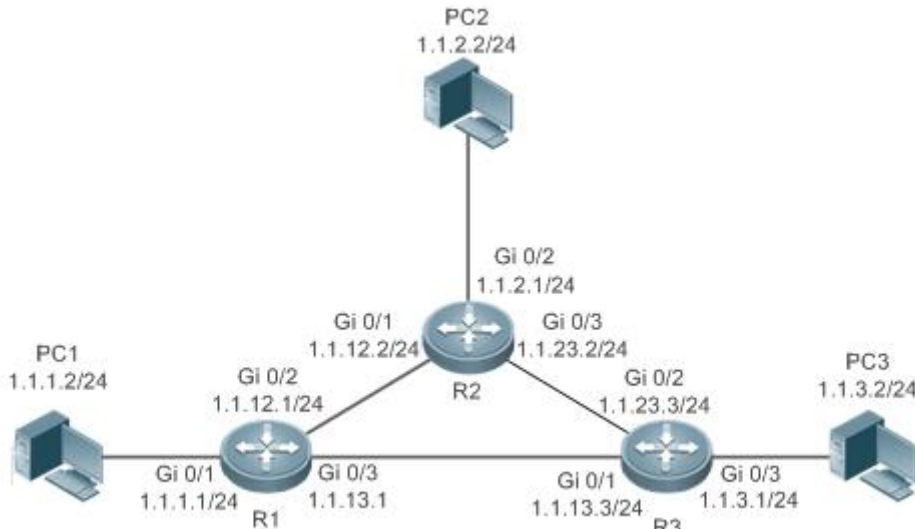
Configuration Steps

▾ [Disabling IPv4 Routing](#)

Command	no ip routing
Parameter	N/A
Description	
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 RGOS software. In this case, you can disable the IPv4 routing function of the RGOS software.

Configuration Example

Configuring at Most Two Static Routing Limitations

<p>Scenario Figure 1-4</p>	
<p>Configuration Steps</p>	<pre> R1#configure terminal R1(config)#interface vlan 1 R1(config-if-VLAN 1)# ip address 1.1.1.1 255.255.255.0 R1(config-if-VLAN 1)# exit R1(config)#interface vlan 2 R1(config-if-VLAN 2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-VLAN 2)# exit R1(config)#interface vlan 3 </pre>

	<pre>R1(config-if-VLAN 3)# ip address 1.1.13.1 255.255.255.0 R1(config-if-VLAN 3)# exit</pre>
Verification	<ul style="list-style-type: none"> ● Check the connected routes that really take effect in the routing table.
	<pre>R1(config)# 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, VLAN 1 C 1.1.1.1/32 is local host. C 1.1.12.0/24 is directly connected, VLAN 2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, VLAN 3 C 1.1.13.1/32 is local host.</pre>

1.4 Monitoring

Clearing

Description	Command
Clears the route cache.	clear ip route { * <i>network</i> [<i>netmask</i>] }

Displaying

Description	Command
Displays the IPv4 routing table.	show ip route
Displays the statistics of the IP routing table	show ip route summary

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 internal events of route management.	debug nsm events
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 IGMP Snooping

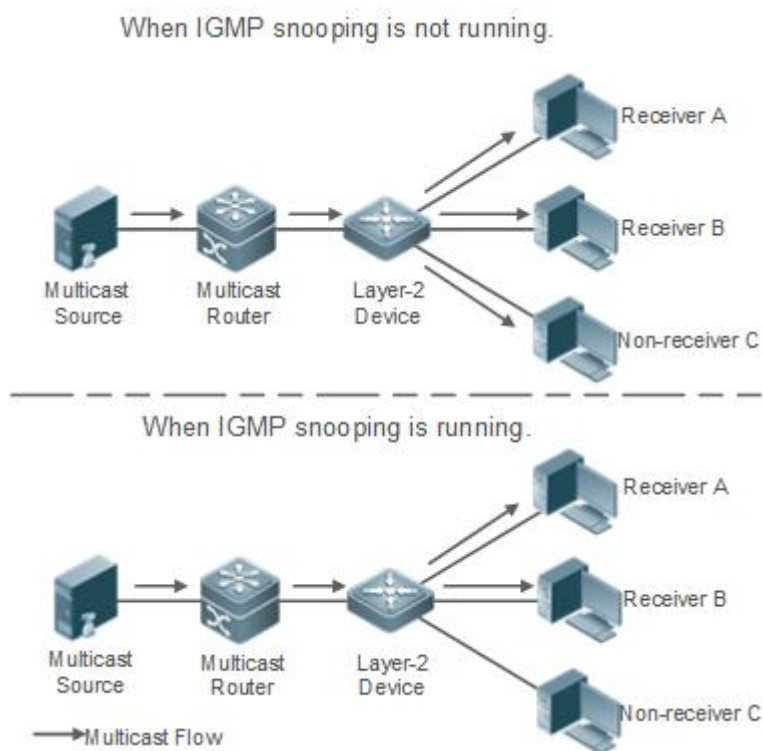
1 Configuring IGMP Snooping

1.1 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 group members.

Figure 1-1 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

1.2 Applications

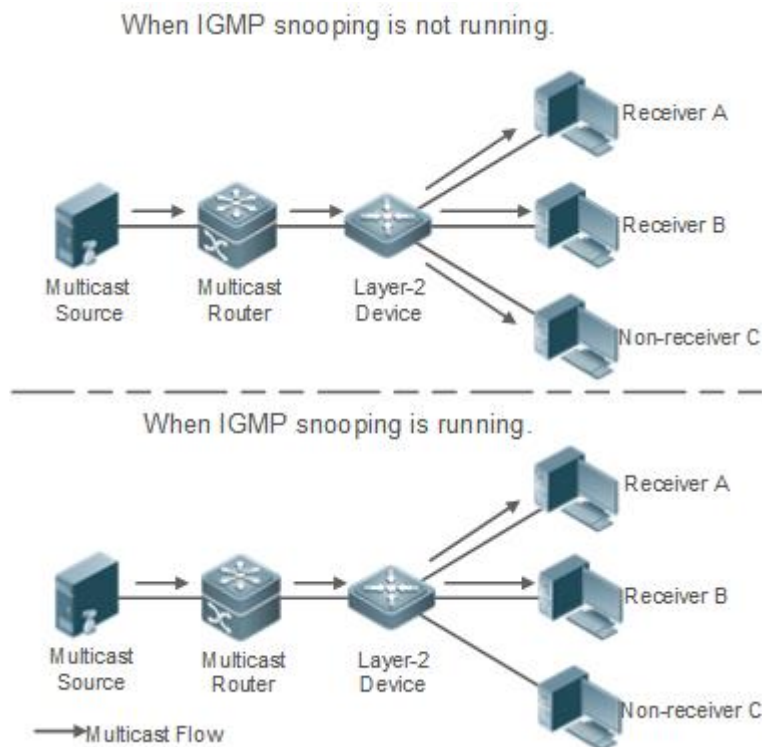
Application	Description
Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Shared Multicast Services (Multicast VLAN)	Multiple users can share the multicast traffic of the same VLAN.
Premium Channels and Preview	Controls the range of multicast addresses that allow user demanding and allows preview for groups who are inhibited from demanding.

1.2.1 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 group will no longer be broadcast within the VLAN but transmitted to designated receivers.

Figure 1-2 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



Deployment

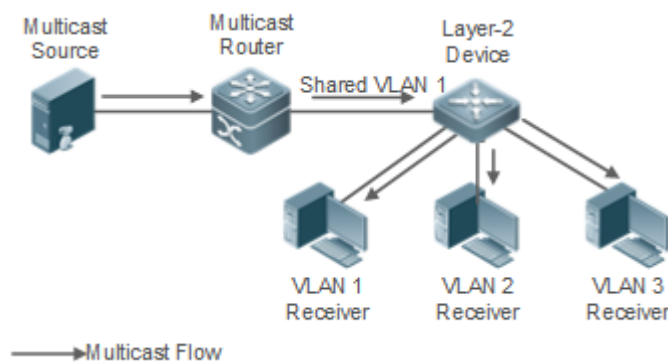
- Configure basic IGMP snooping functions.

1.2.2 Shared Multicast Services (Multicast VLAN)

Scenario

- In Shared VLAN Group Learning (SVGL) mode, 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 1-3 Networking Topology of Shared Multicast Services (Multicast VLAN)



- i** 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).

1.2.3 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 group that are denied access.

1.3 Features

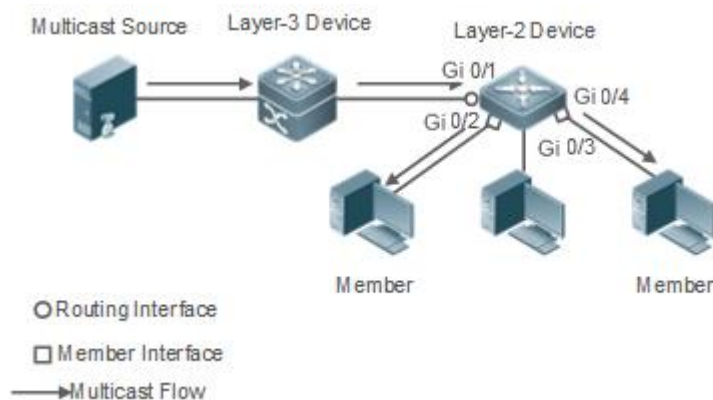
Basic Concepts

↳ Multicast Router Ports and Member Ports

i 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 1-4 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 group 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.

↳ IGMP Snooping Forwarding Entry

The device running IGMP snooping forwards IP multicast packets in accordance with the IGMP snooping forwarding entry.

An IGMP snooping forwarding entry includes the following items: source address (S), group address (G), VLAN ID (VLAN_ID), multicast router port, and member port. It indicates that packets of required features (including S, G, and VLAN_ID) should enter the multicast router port and exit from a member port. An IGMP snooping forwarding entry is identified using a group of S, G, and VLAN_ID.

To display the IGMP snooping forwarding entry, run the **show ip igmp snooping gda-table** command.

```
Ruijie# show ip igmp snooping gda-table
```

Multicast Switching Cache Table

```

D: DYNAMIC //Dynamic member port
S: STATIC //Static member port
M: MROUTE //Multicast router port (dynamic or static)
(*, 233.3.6.29, 1): // (S: any; G: 233.3.6.29; VLAN_ID: VLAN 1)
VLAN(1) 3 OPORTS:
    GigabitEthernet 0/3(S)
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)
(*, 233.3.6.30, 1): // (S: any; G: 233.3.6.30; VLAN_ID: VLAN 1)
VLAN(1) 2 OPORTS:
GigabitEthernet 0/2(M)
GigabitEthernet 0/1(D)

```

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 Profile	Controls the multicast service scope and load to prevent illegal multicast traffic.
IGMP Querier	Defines the range of multicast addresses that permit or deny user requests for reference of other functions.
	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.


1.3.1 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.
- If dynamic router port learning is disabled, IGMP snooping will not learn the dynamic router port.

↘ Report Packets

- i** When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a group, it will also send a report.
- i** By default, IGMP Snooping is capable of processing IGMPv1 and IGMPv2 packets. For IGMPv3 Report packets, it processes group information but does not process carried source information. IGMP Snooping v3 can be configured to process all information in IGMPv1, IGMPv2, and IGMPv3 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 group 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 group.
- 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 group.

↘ Leave Packets

- i** If a host requests to leave a group, 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 group 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 group 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.

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 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.

1.3.2 IGMP Snooping Working Modes

A device running in the two modes (IVGL and 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.

i 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.

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.

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, 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, the number of sub VLANs is not limited.

Configuring an SVGL Group Address Range

No default setting.

Run the **ip igmp snooping svgl profile** *profile_num* command to configure the address range of an SVGL group.

 In SVGL mode, the SVGL group address range must be configured; otherwise, shared multicast services cannot be provided.

1.3.3 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 Group Filtering

By configuring group filtering, 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 user 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 Groups 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 groups allowed for concurrent request can guarantee the bandwidth.

- You can limit the number of groups allowed for concurrent request globally.
- You can also limit the number of groups allowed for concurrent request on a port.

Related Configuration

▾ Configuring the Group Filtering

By default, group filtering is not configured.

To filter multicast groups, 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 groups permitted for multicast preview.

Run the **ip igmp snooping preview interval** to set the multicast preview duration.

↳ Configuring the Maximum Number of Groups Allowed for Concurrent Request on a Port

By default, the number of groups allowed for concurrent request is not limited.

Run the **ip igmp snooping max-groups** command to configure the maximum number of groups allowed for concurrent request.

↳ Configuring the Maximum Number of Multicast Groups Allowed Globally

By default, the maximum number of multicast groups allowed globally is 65,536.

Run the **ip igmp snooping l2-entry-limit** command to configure the maximum number of multicast groups allowed globally.

1.3.4 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.

1.3.5 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 or 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 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. 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 timer expiry** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan querier timer expiry** command to configure the aging time of queriers on specific VLANs.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic IGMP Snooping Functions (IVGL Mode)	 Either of IVGL mode, and 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 <i>num</i>	Disables IGMP snooping for a VLAN.
Configuring Basic IGMP Snooping Functions (SVGL Mode)	 Either of IVGL mode and SVGL mode must be selected. It is used to enable IGMP snooping in SVGL mode.	
	ip igmp snooping svgl	Enables global IGMP snooping in IVGL mode.
	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.
	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL group.
	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.
Configuring the Packet Processing	 (Optional) It is used to adjust relevant configurations for processing protocol packets.	
	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	Configures a static router port.
	p igmp snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type</i> <i>interface-number</i>	Configures a static member port.
	ip igmp snooping vlan <i>vlan-id</i> mrouter learn pim-dvmrp	Enables dynamic router port learning.
	ip igmp snooping dyn-mr-aging-time <i>time</i>	Configures the aging time of a dynamic router port.
	ip igmp snooping host-aging-time <i>time</i>	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 <i>time</i>	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 control security for multicast.	
	ip igmp snooping filter <i>profile-number</i>	Configures the group filtering for user access.
	ip igmp snooping vlan num filter <i>profile-number</i>	Configures the per-VLAN group filtering for user access.
	ip igmp snooping I2-entry-limit <i>number</i>	Configures the maximum number of groups globally for user access.
	ip igmp snooping max-groups <i>number</i>	Configures the maximum number of dynamic groups for user access.
	ip igmp snooping preview <i>profile-number</i>	Enables the preview function for a specified group.
	ip igmp snooping preview interval <i>num</i>	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 <i>profile-number</i>	Creates a profile.
	range <i>low-address high_address</i>	Configures the group address range.
	permit	Permits the access of a user host.
	deny	Denies the access of a user host.
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 <i>num</i>	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan num querier version <i>num</i>	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 <i>num</i>	Configures the query interval of queriers globally.
	ip igmp snooping vlan num querier query-interval <i>num</i>	Configures the query interval for a querier of a VLAN.
ip igmp snooping querier max-response-time <i>num</i>	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.

1.4.1 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	N/A

Description	
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 <i>num</i>
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

<p>Scenario Figure 1-5</p>	
	<p>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.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>A</p>	<pre>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</pre>
<p>B</p>	<pre>B# configure terminal B(config)# ip igmp snooping ivgl</pre>
<p>Verification</p>	<p>Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G.</p> <ul style="list-style-type: none"> ● 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.
<p>B</p>	<pre>B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE</pre>

```
(*, 224.1.1.1, 1):
VLAN(1) 2 OPORTS:
  GigabitEthernet 0/1(M)
  GigabitEthernet 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.

1.4.2 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 groups.

↘ 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	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the SVGL mode is selected, the range of groups within SVGL multicast addresses needs to be associated.

↘ Configuring the SVGL profile

Command	ip igmp snooping svgl profile <i>profile_num</i>
Parameter	<i>profile_num</i> : Configures SVGL to associate a profile.
Description	
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 <i>vid</i>
Parameter	<i>vid</i> : Indicates a VLAN.
Description	

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 <i>vid-range</i>
Parameter Description	<i>vid-range</i> : 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**

<p>Scenario Figure 1-6</p>	
	<p>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.</p>
Configuration	<ul style="list-style-type: none"> Configure the IP address and VLAN. (Omitted)

Steps	<ul style="list-style-type: none"> ● 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	<pre>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</pre>
B	<pre>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</pre>
Verification	<p>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.</p> <ul style="list-style-type: none"> ● 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	<pre>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</pre>

```
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 group is not configured.
- The sent multicast traffic is not within the SVGL group.

1.4.3 Configuring the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all groups.
- Configure specified ports as the static member ports to receive the multicast traffic from specified groups
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or group 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.
- Configure IGMP Snooping V3 to process all information in IGMPv3 packets.

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 group, 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 <i>vid</i> mrouter interface <i>interface-type interface-number</i>
Parameter	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094.
Description	<i>interface-type interface-number</i> : 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 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 <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i>
Parameter	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094.
Description	<i>group-address</i> : Indicates a group address. <i>interface-type interface-number</i> : 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	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or group 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, and the IGMPv3 Report packets cannot 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	<p>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 groups. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address.</p> <p>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.</p>

▾ Enabling Dynamic Router Port Learning

Command	ip igmp snooping [vlan <i>vid</i>] mrouter learn pim-dvmrp
Parameter Description	 vlan <i>vid</i> : 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 <i>seconds</i>
Parameter Description	 <i>seconds</i> : 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	<p>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.</p> <p>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.</p>

▾ Configuring the Aging Time of a Dynamic Member Port

Command	ip igmp snooping host-aging-time <i>seconds</i>
Parameter Description	 <i>seconds</i> : Indicates the aging time.
Command Mode	Global configuration mode

Usage Guide	<p>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 group.</p> <p>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.</p>
--------------------	--

▾ Configuring the Maximum Response Time of a Query Packet

Command	ip igmp snooping query-max-response-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the maximum response time.
Command Mode	Global configuration mode
Usage Guide	N/A

▾ Displaying Router Ports

Command	show ip igmp snooping mrouter
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the router port is successfully configured, an "S" will be displayed in the port information.</p> <pre>Ruijie(config)#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)</pre>

▾ 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	<p>Run the show ip igmp snooping command to display the aging time and learning status of the dynamic router port.</p> <pre>Dynamic Mroute Aging Time : 300(Seconds)</pre>

	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	<p>If the member port is successfully configured, an "S" will be displayed in the port information.</p> <pre>Ruijie(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)</pre>

▾ 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	<p>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.</p> <pre>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)</pre>

Configuration Example

▾ Configuring a Static Router Port and Static Member Port

Configuration Steps	<ul style="list-style-type: none"> ● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
----------------------------	--

	<pre>Ruijie# configure terminal Ruijie(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/1 Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/1 Ruijie(config)# end</pre>
Verification	<p>Run the show ip igmp snooping mrouter and show ip igmp snooping gda-table commands to check whether the configuration takes effect.</p>
	<pre>Ruijie#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S) Ruijie#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(SM)</pre>

➤ **Enabling Report Packet Suppression**

<p>Scenario Figure 1-7</p>	<p>The diagram illustrates a network topology for IGMP snooping configuration. At the top, a server labeled 'Source 1' with IP 10.1.1.1/24 is connected to 'Device A' (a multicast router) via its Gi 0/1 interface. Device A's Gi 0/2 interface is connected to 'Device B' (a Layer-2 switch) via its Gi 0/1 interface. Device B has three other interfaces: Gi 0/2 connected to 'Receiver 1', Gi 0/3 connected to 'Receiver 2', and Gi 0/4 connected to 'Receiver 3'. Both Device A and Device B are configured with VLAN 1, and the IP address 192.168.1.1 is shown on Device B's Gi 0/1 interface.</p>
	<p>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.</p>

Configuration Steps	<ul style="list-style-type: none"> ● 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	<pre>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</pre>
B	<pre>B# configure terminal B(config)# ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable</pre>
Verification	<p>Check whether Receiver 1 and Receiver 2 are added to group 239.1.1.1, and only the IGMP Report packets of group 239.1.1.1 are forwarded from interface Gi0/1 of B.</p>
B	<pre>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)</pre>

📌 Configuring Other Parameters

Configuration Steps	<ul style="list-style-type: none"> ● 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.
----------------------------	---

	<pre> Ruijie# configure terminal Ruijie(config)# ip igmp snooping fast-leave enable Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp Ruijie(config)#ip igmp snooping dyn-mr-aging-time 200 Ruijie(config)#ip igmp snooping host-aging-time 100 Ruijie(config)#ip igmp snooping query-max-response-time 60 Ruijie(config)# end </pre>
Verification	Run the show ip igmp snooping command to check whether the configuration is successful.
	<pre> Ruijie#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) </pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

1.4.4 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 group 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 Group Filtering

- Optional.
- If you want to limit the group packets received by a port, you can configure the group filtering on the port.
- If you want to limit the group packets received by a VLAN, you can configure the group filtering on the VLAN.

▾ Enabling Multicast Preview

- Optional.
- You can enable multicast preview for a user from an unauthorized group.

▾ Configuring the Maximum Number of Groups

- Optional.
- If you want to limit the number of multicast groups that a port is allowed to receive, you can configure the maximum number of multicast groups allowed for this port.
- If you want to limit the number of multicast groups that global ports are allowed to receive, you can configure the maximum number of multicast groups allowed for these ports.

Verification

- Run the **show ip igmp snooping interfaces** command to display the group filtering and the maximum number of multicast profiles for a port.
- Run the **show ip igmp snooping vlan** command to display the VLAN-based group filtering.
- Run the **show ip igmp snooping** command to check whether the maximum number of global multicast groups, preview function, source port inspection, and source IP address inspection take effect.

Related Commands

▾ Configuring the Profile Filtering

Command	ip igmp snooping filter <i>profile-number</i>
Parameter Description	<i>profile-number</i> : Indicates a profile number.
Command Mode	Interface configuration mode
Usage Guide	N/A

▾ Configuring the Per-VLAN Group Filtering

Command	ip igmp snooping vlan <i>vid filter profile-number</i>
Parameter Description	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094. <i>profile-number</i> : Indicates a profile number.

Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Maximum Number of Groups on a Port

Command	ip igmp snooping max-groups <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of multicast groups.
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 Groups

Command	ip igmp snooping l2-entry-limit <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of multicast groups.
Command Mode	Global configuration mode
Usage Guide	This value includes the number of both dynamic groups as well as static groups.

↘ Enabling Preview

Command	ip igmp snooping preview <i>profile-number</i>
Parameter Description	<i>profile number</i> : 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 <i>num</i>
Parameter Description	<i>num</i> : 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 Port-based Group 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	<p>If the function is configured, the group will be displayed, for example:</p> <pre>Ruijie#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ----- GigabitEthernet 0/1 1</pre>

▾ Displaying the VLAN-based Group 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	<p>If the function is configured, the group will be displayed, for example:</p> <pre>IGMP VLAN filter: 1</pre>

▾ Displaying the Maximum Number of Interface Groups

Command	show ip igmp snooping interface
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the maximum number of multicast addresses for a port is configured, the value will be displayed, for example:</p> <pre>Ruijie#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ----- GigabitEthernet 0/1 1 200</pre>

▾ Displaying the Maximum Number of Global Groups

Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the function is configured, the profile will be displayed, for example:</p> <pre>IGMP Snooping L2-entry-limit: 65536</pre>

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: <pre>IGMP Preview: Enable IGMP Preview group aging time : 60(Seconds)</pre>

Configuration Example

Configuring the Group Filtering and the Maximum Number of Demanded Groups

<p>Scenario</p> <p>Figure 1-8</p>	
	<p>A is the multicast router and is connected directly to multicast Source 1.</p> <p>B is a Layer-2 device and is connected directly to the user host and multicast Source 2.</p> <p>Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.</p> <p>By configuring VLAN 1, you can configure to allow the users within VLAN 1 to receive only the groups whose addresses range from 225.1.1.1 to 225.1.255.255.</p> <p>You can configure Receiver 1 to receive only the groups whose addresses range from 225.1.1.1 to 225.1.1.255, Receiver 2 to receive only the groups whose addresses range from 225.1.2.1 to 255.1.2.255, and Receiver 3 to receive only the groups whose addresses range from 225.1.3.1 to 225.1.3.255.</p> <p>At most 10 groups can be added to a port and at most 100 groups can be added globally.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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	<pre> 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 </pre>
B	<pre> 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 B(config-if-GigabitEthernet 0/2)#ip igmp snooping filter 2 B(config-if-GigabitEthernet 0/2)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ip igmp snooping filter 3 B(config-if-GigabitEthernet 0/3)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/4 B(config-if-GigabitEthernet 0/4)#ip igmp snooping filter 4 B(config-if-GigabitEthernet 0/4)#ip igmp snooping max-groups 10 </pre>
Verification	<ul style="list-style-type: none"> ● Run the show ip igmp snooping interfaces command to display the group filtering and the maximum number of multicast groups for a port.

	<ul style="list-style-type: none"> Run the show ip igmp snooping command to display the maximum number of global multicast groups.
B	<pre> 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) </pre>

1.4.5 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 <i>profile-number</i>
Parameter	<i>profile-number</i> : Indicates the number of a profile.
Description	
Command Mode	Global configuration mode
Usage Guide	

↳ Configuring the Group Address Range

Command	range <i>low-ip-address</i> [<i>high-ip-address</i>]
Parameter	<i>low-ip-address</i> : Specifies the start address.
Description	<i>low-ip-address</i> : 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 address ranges are overlapped, the addresses will be combined.

↳ Configuring Group Filtering

Command	deny
Parameter	N/A
Description	
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode is set to deny while the group address range is not specified, no group will be denied.

↳ Configuring Group Filtering

Command	permit
Parameter	N/A
Description	
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode is set to permit while the group address range is not specified, no group will be permitted.

Configuration Example

↳ Creating a Filtering Profile

Configuration Steps	<ul style="list-style-type: none"> ● Create a filtering profile.
----------------------------	---

	<pre>Ruijie(config)#ip igmp profile 1 Ruijie(config-profile)#permit Ruijie(config-profile)#range Ruijie(config-profile)#range 224.1.1.1 235.1.1.1 Ruijie(config-profile)#</pre>
Verification	Run the show running-config command to check whether the configuration is successful.
	<pre>ip igmp profile 1 permit range 224.1.1.1 235.1.1.1 !</pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.
- The filtering mode is set to permit while the group address range is not specified, leading to the denial of all groups.

1.4.6 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 <i>vid</i>] querier
Parameter Description	vlan <i>vid</i> : 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 <i>vid</i>] querier address <i>a.b.c.d</i>
Parameter Description	vlan <i>vid</i> : Specifies a VLAN. This configuration applies to all VLANs by default. <i>a.b.c.d</i> : 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 <i>vid</i>] querier max-response-time <i>seconds</i>
Parameter Description	vlan <i>vid</i> : Specifies a VLAN. This configuration applies to all VLANs by default. <i>seconds</i> : 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 query-interval seconds
Parameter	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Description	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	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Description	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 2 }
Parameter	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Description	
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

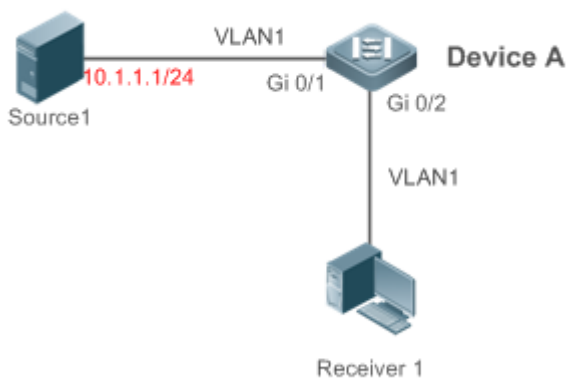
Command	show ip igmp snooping querier detail
Parameter	N/A
Description	
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed. <pre>Ruijie(config)#show ip igmp snooping querier detail Vlan IP Address IGMP Version Port ----- Global IGMP switch querier status -----</pre>

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

<p>Scenario Figure 1-9</p>	
	<p>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.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Enable global IGMP snooping on A in IVGL mode. ● Enable IGMP querier for VLAN 1 on A.
<p>A</p>	<pre>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</pre>

Verification	Run the show ip igmp snooping querier command to check whether the querier of VLAN 1 takes effect.
A	<pre> 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 </pre>

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

1.5 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 <i>vlan-id</i>]
Displays the statistics on IGMP snooping.	show ip igmp snooping statistics [vlan <i>vlan-id</i>]
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 [<i>profile-number</i>]
Displays the IGMP snooping configurations on an interface.	show ip igmp snooping interface <i>interface-name</i>
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 Storm Control
3. Configuring Password Policy
4. Configuring Port Security
5. Configuring SSH
6. Configuring CPU Protection
7. Configuring DHCP Snooping
8. Configuring ACL
9. Configuring QoS

1 Configuring AAA

 S1930J series switches do not support remote server authentication.

1.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring the authentication, authorization, and accounting services. Ruijie Networks 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. Ruijie Networks also provides 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.

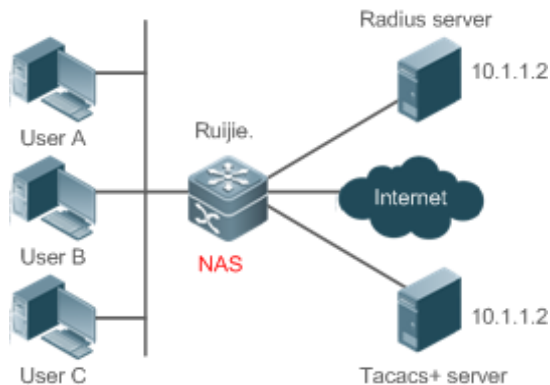
1.2.1 Configuring AAA in a Single-Domain Environment

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	<p>The NAS is an access or convergence switch.</p> <p>The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor.</p> <p>The TACACS+ server can be the dedicated server software provided by a vendor.</p>
----------------	--

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.

1.3 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 Ruijie 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 Ruijie 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 Ruijie devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 1-2

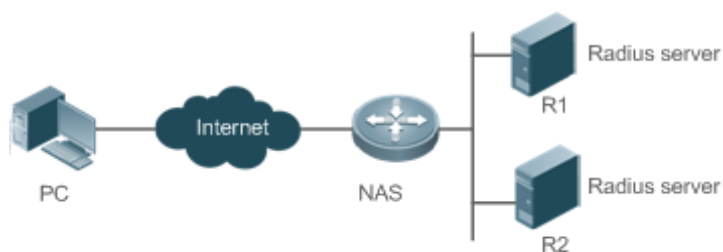




Figure 1-2 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

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+*.

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.

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** 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

Ruijie 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).

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 getting 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.

1.4 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.
	login authentication	Enables login authentication on a specific terminal line.
	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.
	accounting exec	Applies EXEC accounting methods to a specified VTY line.

Configuration	Description and Command	
	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 AAA Logging	aaa log enable	Enables AAA logging.
	aaa log rate-limit	Configures AAA logging rate limit.

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.
-
- i** 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.

↘ Enabling Login Authentication on a Specific Terminal Line

- Run the **login authentication** command in line mode to apply login authentication to a specific terminal line.
- This configuration is mandatory if you need to enable the login authentication method list on a specific terminal line.
- By default, no method list of Enable 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.

Related Commands

↘ Enabling AAA

Command	aaa new-model
Parameter	N/A
Description	
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	default: With this parameter used, the configured method list will be defaulted.
Description	<p><i>list-name:</i> Indicates the name of a login authentication method list in characters.</p> <p><i>method:</i> Indicates authentication methods from local, none, group. A method list contains up to four methods.</p> <p>local: Indicates that the local user database is used for authentication.</p> <p>none: Indicates that authentication is not performed.</p> <p>group: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>In a method list, the next method is executed only when the current method does not receive response.</p> <p>After you configure login authentication methods, apply the methods to the VTY lines that require login authentication; otherwise, the methods will not take effect.</p>

▾ Defining a Method List of Enable Authentication

Command	aaa authentication enable default method1 [method2...]
Parameter	default: With this parameter used, the configured method list will be defaulted.
Description	<p><i>list-name:</i> Indicates the name of an Enable authentication method list in characters.</p> <p><i>method:</i> Indicates authentication methods from enable, local, none, and group. A method list contains up to four methods.</p> <p>enable: Indicates that the password that is configured using the enable command is used for authentication.</p> <p>local: Indicates that the local user database is used for authentication.</p> <p>none: Indicates that authentication is not performed.</p> <p>group: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>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</p>

	<p>method lists for Enable authentication.</p> <p>In a method list, the next method is executed only when the current method does not receive response.</p>
--	---

▾ **Setting the Maximum Number of Login Attempts**

Command	aaa local authentication attempts <i>max-attempts</i>
Parameter Description	<i>max-attempts</i> : 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 <i>lockout-time</i>
Parameter Description	<i>lockout-time</i> : Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 43,200, 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 1-3	<p>The diagram shows a User laptop on the left connected to a Network Access Server (NAS) in the middle via interface Gi 0/1. The NAS is then connected to a Server on the right via interface Gi 0/2. The Server's IP address is 10.1.1.1.</p>
Configuration Steps	<p>Step 1: Enable AAA.</p> <p>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.)</p> <p>Step 3: Configure an AAA authentication method list for login authentication users. (This example uses group <i>radius</i> and local in order.)</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.</p>
NAS	<pre>Ruijie#configure terminal Ruijie(config)#username user password pass</pre>

	<pre>Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key ruijie Ruijie(config)#aaa authentication login list1 group radius local Ruijie(config)#line vty 0 20 Ruijie(config-line)#login authentication list1 Ruijie(config-line)#exit</pre>
Verification	Run the show aaa method-list command on the NAS to display the configuration.
NAS	<pre>Ruijie#show aaa method-list Authentication method-list: aaa authentication login list1 group radius local Accounting method-list: Authorization method-list:</pre>
	<p>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.</p> <p>The user must enter the correct username and password to access the NAS.</p>
User	<pre>User Access Verification Username:user Password:pass</pre>

📌 **Configuring AAA Enable Authentication**

Configure an Enable authentication method list on the NAS containing **group radius**, **local**, and then **enable** methods in order.

<p>Scenario Figure 1-4</p>	<pre> graph LR User[User] --- Gi01[Gi 0/1] --- NAS[NAS] NAS --- Gi02[Gi 0/2] --- Server[Server 10.1.1.1] </pre>
Configuration	Step 1: Enable AAA.

Steps	<p>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.</p> <p>Step 3: Configure an AAA authentication method list for Enable authentication users.</p> <hr/> <p> 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.</p> <hr/>
NAS	<pre>Ruijie#configure terminal Ruijie(config)#username user privilege 15 password pass Ruijie(config)#enable secret w Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key ruijie Ruijie(config)#aaa authentication enable default group radius local enable</pre>
Verification	Run the show aaa method-list command on the NAS to display the configuration.
NAS	<pre>Ruijie#show aaa method-list Authentication method-list: aaa authentication enable default group radius local enable Accounting method-list: Authorization method-list:</pre>
	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	<pre>Ruijie>enable Username:user Password:pass Ruijie#</pre>

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: The RGOS 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	N/A

Description	
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 <i>list-name</i> } <i>method1</i> [<i>method2...</i>]
Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of an EXEC authorization method list in characters.</p> <p><i>method:</i> Specifies authentication methods from local, none, and group. A method list contains up to four methods.</p> <p>local: Indicates that the local user database is used for EXEC authorization.</p> <p>none: Indicates that EXEC authorization is not performed.</p> <p>group: Indicates that a server group is used for EXEC authorization. Currently, the RADIUS and TACACS+ server groups are supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>The RGOS 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.</p> <p>After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.</p>

▾ Defining a Method List of Command Authorization

Command	aaa authorization commands <i>level</i> { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]
Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of a command authorization method list in characters.</p> <p><i>method:</i> Indicates authentication methods from none, group and local. A method list contains up to four methods.</p> <p>none: Indicates that command authorization is not performed.</p> <p>group: Indicates that a server group is used for command authorization. Currently, the TACACS+ server group is supported.</p> <p>local: Indicates that a local user name database is used for command authorization.</p>
Command Mode	Global configuration mode
Usage Guide	<p>The RGOS 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.</p>

	<p>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.)</p> <p>After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.</p>
--	---

▾ Configuring a Method List of Network Authorization

Command	aaa authorization network { default list-name } method1 [method2...]
Parameter Description	<p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name:</i> Indicates the name of a network authorization method list in characters.</p> <p><i>method:</i> Indicates authentication methods from none and group. A method list contains up to four methods.</p> <p>none: Indicates that authentication is not performed.</p> <p>group: Indicates that a server group is used for network authorization. Currently, the RADIUS and TACACS+ server groups are supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>The RGOS 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.</p> <p>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.</p> <p>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.</p>

▾ 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	The RGOS 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 1-5	<pre> graph LR User[User] --- Gi01[Gi 0/1] --- NAS[NAS] NAS --- Gi02[Gi 0/2] --- Server[Server] subgraph Server_IP [10.1.1.1] Server end </pre>
Configuration Steps	<p>Step 1: Enable AAA.</p> <p>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.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p> <p>EXEC authorization is often used with login authentication, which can be implemented on the same line.</p>
NAS	<pre> Ruijie#configure terminal Ruijie(config)#username user password pass Ruijie(config)#username user privilege 6 Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key test Ruijie(config)#aaa authentication login list1 group local Ruijie(config)#aaa authorization exec list2 group radius local Ruijie(config)#line vty 0 4 Ruijie(config-line)#login authentication list1 Ruijie(config-line)# authorization exec list2 Ruijie(config-line)#exit </pre>

Verification	Run the show run and show aaa method-list commands on the NAS to display the configuration.
NAS	<pre>Ruijie#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</pre>
	<pre>Ruijie# 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</pre>

📌 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.

<p>Scenario Figure 1-6</p>	
<p>Configuration Steps</p>	<p>Step 1: Enable AAA.</p> <p>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.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p> <p>Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.</p>
<p>NAS</p>	<pre>Ruijie#configure terminal Ruijie(config)#username user1 password pass1 Ruijie(config)#username user1 privilege 15 Ruijie(config)#aaa new-model Ruijie(config)#tacacs-server host 10.1.1.1 Ruijie(config)#tacacs-server key aaa Ruijie(config)#aaa authentication login default local Ruijie(config)#aaa authorization commands 15 default group tacacs+ local Ruijie(config)#aaa authorization console</pre>
<p>Verification</p>	<p>Run the show run and show aaa method-list commands on the NAS to display the configuration.</p>
<p>NAS</p>	<pre>Ruijie#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</pre>
	<pre>Ruijie#show run ! aaa new-model</pre>

```

!
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 10.1.1.1
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
    
```

➤ **Configuring AAA Network Authorization**

<p>Scenario Figure 1-7</p>	
<p>Configuration Steps</p>	<p>Step 1: Enable AAA.</p> <p>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.</p> <p>Step 3: Configure an AAA authorization method list according to different access modes and service types.</p>

	Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	<pre>Ruijie#configure terminal Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key test Ruijie(config)#aaa authorization network default group radius none Ruijie(config)# end</pre>
Verification	Run the show aaa method-list command on the NAS to display the configuration.
NAS	<pre>Ruijie#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none</pre>

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.

↳ 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.

↘ 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	N/A
Description	
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	default: With this parameter used, the configured method list will be defaulted.
Description	<i>list-name:</i> Indicates the name of an EXEC accounting method list in characters. <i>method:</i> 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	Global configuration mode

Mode	
Usage Guide	<p>The RGOS 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.</p> <p>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.</p> <p>After you configure EXEC accounting methods, apply the methods to the VTY lines that require EXEC accounting; otherwise, the methods will not take effect.</p>

▾ Defining a Method List of Command Accounting

Command	aaa accounting commands <i>level</i> { default <i>list-name</i> } start-stop <i>method1</i> [<i>method2...</i>]
Parameter Description	<p><i>level</i>: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15.</p> <p>After a command of the configured level is executed, the accounting server records related information based on the received accounting packet.</p> <p>default: With this parameter used, the configured method list will be defaulted.</p> <p><i>list-name</i>: Indicates the name of a command accounting method list in characters.</p> <p><i>method</i>: Indicates authentication methods from none and group. A method list contains up to four methods.</p> <p>none: Indicates that command accounting is not performed.</p> <p>group: Indicates that a server group is used for command accounting. Currently, the TACACS+ server group is supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>The RGOS 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.</p> <p>After you configure command accounting methods, apply the methods to the VTY lines that require command accounting; otherwise, the methods will not take effect.</p>

▾ 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 <i>interval</i>
----------------	---

Parameter Description	<i>Interval</i> : Indicates the accounting update interval, in the range from 1 to 525,600, in the unit of minutes.
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 1-8	
Configuration Steps	<p>Step 1: Enable AAA.</p> <p>If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance.</p> <p>Step 2: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.</p>
NAS	<pre>Ruijie#configure terminal Ruijie(config)#username user password pass Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key test Ruijie(config)#aaa authentication login list1 group local Ruijie(config)#aaa accounting exec list3 start-stop group radius Ruijie(config)#line vty 0 4 Ruijie(config-line)#login authentication list1 Ruijie(config-line)# accounting exec list3 Ruijie(config-line)#exit</pre>
Verification	Run the show run and show aaa method-list commands on the NAS to display the configuration.
NAS	<pre>Ruijie#show aaa method-list</pre>

	<pre>Authentication method-list: aaa authentication login list1 group local Accounting method-list: aaa accounting exec list3 start-stop group radius Authorization method-list:</pre>
	<pre>Ruijie# 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</pre>

↘ 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.



Configuration Steps	<p>Step 1: Enable AAA.</p> <p>If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance.</p> <p>Step 2: Configure an AAA accounting method list according to different access modes and service types.</p> <p>Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.</p>
NAS	<pre>Ruijie#configure terminal Ruijie(config)#username user1 password pass1 Ruijie(config)#username user1 privilege 15 Ruijie(config)#aaa new-model Ruijie(config)#tacacs-server host 10.1.1.1 Ruijie(config)#tacacs-server key aaa Ruijie(config)#aaa authentication login default local Ruijie(config)#aaa accounting commands 15 default start-stop group tacacs+</pre>
Verification	<p>Run the show aaa method-list command on the NAS to display the configuration.</p>
NAS	<pre>Ruijie#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:</pre>
	<pre>Ruijie#show run ! aaa new-model ! aaa authorization config-commands aaa accounting commands 15 default start-stop group tacacs+ aaa authentication login default local</pre>

```
!  
!  
nfpp  
!  
vlan 1  
!  
username user1 password 0 pass1  
username user1 privilege 15  
no service password-encryption  
!  
tacacs-server host 10.1.1.1  
tacacs-server key aaa  
!  
line con 0  
line vty 0 4  
!  
!  
end
```

Common Errors

N/A

1.4.4 Configuring AAA Logging

Configuration Effect

- When users pass AAA authentication, the device will output logs. Configure this function to disable AAA logging or configure AAA logging rate limit.

Notes

N/A

Configuration Steps

▾ Enable AAA Logging

- AAA logging is enabled by default.

➤ **Configuring AAA Logging Rate Limit**

- The default rate limit is 5 syslogs per second.

Verification

Run the **show run** command to verify the configuration.

Related Commands

➤ **Enabling AAA Logging**

Command	<code>[no] aaa log enable</code>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Too much printing may flood the screen or even reduce device performance. In this case, use this command to disable logging.

➤ **Configuring AAA Logging Rate Limit**

Command	<code>aaa log rate-limit num</code> <code>no aaa log rate-limit</code>
Parameter Description	<i>num</i> : The number of syslog entries printed per second. The range is from 0 to 65,535. 0: 0 indicates no rate limit is configured. The range is from 0 to 65,535. The default rate limit is 5 syslogs per second.
Command Mode	Global configuration mode
Usage Guide	Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the locked users.	<code>clear aaa local user lockout { all user-name username }</code>

Displaying

Description	Command
-------------	---------

Displays the accounting update information.	show aaa accounting update
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 Storm Control

2.1 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.

2.2 Applications

Application	Description
Network Attack Prevention	Enable storm control to prevent flooding.

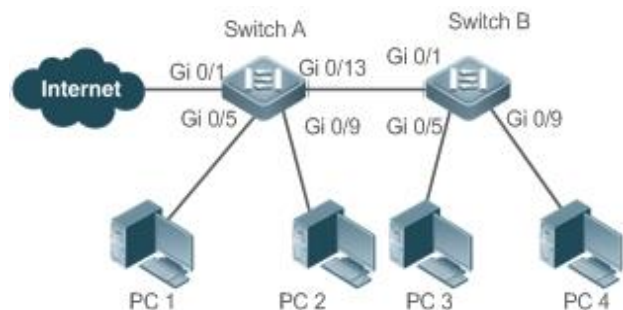
2.2.1 Network Attack Prevention

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 2-1



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).

2.3 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.

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.4 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 <i>percent</i> pps <i>packets</i> <i>rate-bps</i>] Enables storm control.

2.4.1 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 unicast**) 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 [<i>level percent</i> pps packets <i>rate-bps</i>]
Parameter Description	level percent : Indicates the bandwidth percentage. pps packets : Indicates the number of packets per second. <i>rate-bps</i> : Indicates the packet rate, in the range from 64 to 1,000,000.
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 [<i>level percent</i> pps packets <i>rate-bps</i>]
Parameter Description	level percent : Indicates the bandwidth percentage. pps packets : Indicates the number of packets per second. <i>rate-bps</i> : Indicates the packet rate, in the range from 64 to 1,000,000.
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 [<i>level percent</i> pps packets <i>rate-bps</i>]
Parameter Description	level percent : Indicates the bandwidth percentage. pps packets : Indicates the number of packets per second. <i>rate-bps</i> : Indicates the packet rate, in the range from 64 to 1,000,000.
Command Mode	Interface configuration mode
Usage Guide	Storm control can be enabled only on switch ports.

Configuration Example

➤ **Enabling Storm Control on Devices**

Scenario	
-----------------	--

<p>Figure 2-1</p>	
<p>Configuration Step</p>	<ul style="list-style-type: none"> ● Enable storm control on Switch A and Switch B.
<p>Switch A</p>	<pre>Ruijie(config)#interface range gigabitEthernet 0/5,0/9,0/13 Ruijie(config-if-range)#storm-control broadcast Ruijie(config-if-range)#storm-control multicast Ruijie(config-if-range)#storm-control unicast</pre>
<p>Switch B</p>	<pre>Ruijie(config)#interface range gigabitEthernet 0/1,0/5,0/9 Ruijie(config-if-range)#storm-control broadcast Ruijie(config-if-range)#storm-control multicast Ruijie(config-if-range)#storm-control unicast</pre>
<p>Verification</p>	<p>Check whether storm control is enabled on Switch A and Switch B.</p>
<p>Switch A</p>	<pre>Ruijie# show storm-control Interface Broadcast Control Multicast Control Unicast Control Action ----- GigabitEthernet 0/1 Disabled Disabled Disabled none GigabitEthernet 0/5 default default default none GigabitEthernet 0/9 default default default none GigabitEthernet 0/13 default default default none</pre>
<p>Switch B</p>	<pre>Ruijie#show storm-control Interface Broadcast Control Multicast Control Unicast Control Action ----- GigabitEthernet 0/1 default default default none GigabitEthernet 0/5 default default default none</pre>

	GigabitEthernet 0/9	default	default	default	none
--	---------------------	---------	---------	---------	------

2.5 Monitoring

Displaying

Description	Command
Displays storm control information.	show storm-control [<i>interface-type interface-number</i>]

3 Configuring Password Policy

3.1 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

3.2 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.

↘ **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.

3.3 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.
	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 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.

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	password policy life-cycle <i>days</i>
Parameter	life-cycle <i>days</i> : Indicates the password life cycle in the unit of days. The value range is from 1 to 65535.

Description	
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	password policy min-size <i>length</i>
Parameter Description	min-size <i>length</i> : 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	password policy no-repeat-times <i>times</i>
Parameter Description	no-repeat-times <i>times</i> : 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 the Strong Password Detection Function

Command	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: <ol style="list-style-type: none"> 1. Passwords that are the same as corresponding accounts; 2. Simple passwords that contain characters or digits only.

Setting the Storage of Encrypted Passwords

Command	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	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.

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: <ol style="list-style-type: none"> 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.
Configuration Steps	<ul style="list-style-type: none"> ● 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 the password dictionary detection function. <pre>Ruijie# configure terminal</pre>

	<pre>Ruijie(config)# password policy min-size 8 Ruijie(config)# password policy life-cycle 90 Ruijie(config)# service password-encryption Ruijie(config)# password policy no-repeat-times 3 Ruijie(config)# password policy strong</pre>
Verification	<p>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.</p> <ul style="list-style-type: none"> ● Run the show password policy command to display user-configured password security policy information. <pre>Ruijie# show password policy Global password policy configurations: Password encryption: Enabled Password strong-check: 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)</pre>

Common Errors

- The time configured for giving a pre-warning notice about password expiry to the user is greater than the password life cycle.

3.4 Monitoring

Displaying

Description	Command
Displays user-configured password security policy information.	show password policy

4 Configuring Port Security

4.1 Overview

Port security is used to restrict access to a port. Source MAC addresses of packets can be used to restrict the packets that enter the ports of a switch. You can set the number of static MAC addresses or the number of MAC addresses that are dynamically learned to restrict the packets that can enter the port. Ports enabled with port security are called secure ports.

4.2 Applications

Application	Description
Allowing Only Specified Hosts to Use Ports	For network security, certain ports of a device can be used only by specified hosts.

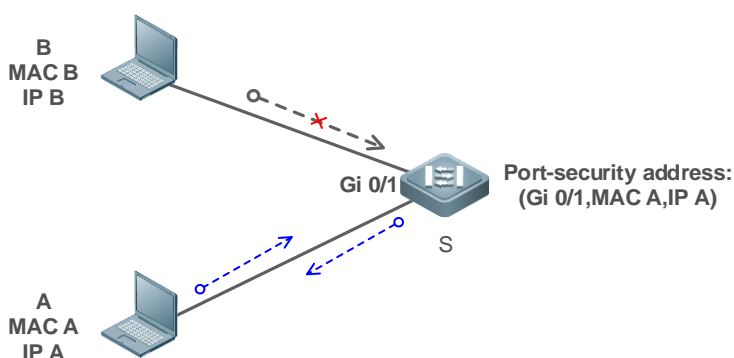
4.2.1 Allowing Only Specified Hosts to Use Ports

Scenario

In a scenario that has requirements for the network security, devices cannot be completely isolated physically. In this case, the devices need to be configured to restrict the PCs that connected to the ports of the devices.

- Only specified PCs can connect to the ports and normally use the network.
- Other PCs cannot use the network even if connected to the ports.
- After the configuration is complete, the administrator does not need to perform regular maintenance.

Figure 4-1



Remark	S is the access device.
s	A is a PC that can use the port Gi 0/1. B is an unknown PC.

Deployment

- Enable ARP Check for port Gi 0/1 (omitted).

- Enable port security on access device S and set the violation handling mode to protect.
- Configure a static port security address on the port Gi 0/1.

4.3 Features

Basic Concepts

Secure Port

Ports configured with port security are called secure ports. At present, Ruijie devices require that secure ports cannot be destination ports of mirroring.

Secure Addresses

Addresses bound to secure ports are called secure addresses. Secure addresses can be layer-2 addresses, namely MAC addresses, and can also be layer-3 addresses, namely, IP or IP+MAC addresses. When a secure address is bound to IP+MAC and a static secure MAC address is configured, the static secure MAC address must be the same as the MAC address bound to IP+MAC; otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP binding is set, only packets whose secure MAC addresses are statically configured or learned and whose source IP addresses are the bound IP address can enter the device.

Dynamic Binding

A method for a device to automatically learn addresses and convert learned addresses into secure addresses.

Static Binding

A command for manually binding secure addresses.

Aging of Secure Addresses

Regularly delete secure address records. Secure addresses for port security support aging configuration. You can specify only dynamically learned addresses for aging or specify both statically configured and dynamically learned secure addresses for aging.

Security Violation Events

When the number of learned MAC addresses learned by a port exceeds the maximum number of secure addresses, security violation events will be triggered. You can configure the following modes for handling security violation events:

- protect: When security violation occurs, a corresponding secure port will stop learning MAC addresses and discard all packets of newly accessed users. This is the default mode for handling violation.
- restrict: When violation occurs, a port violation trap notification will be sent in addition to the behavior in the protect mode.
- shutdown: When violation occurs, the port will be disabled in addition to the behaviors in the preceding two modes.

Maximum Number of Secure Addresses

The maximum number of secure addresses indicates the total number of secure addresses statically configured and dynamically learned. When the number of secure addresses under a secure port does not reach the maximum number

of secure addresses, the secure port can dynamically learn new dynamic secure addresses. When the number of secure addresses reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. If new users access the secure port in this case, security violation events will occur. On the device, the maximum number of secure addresses of a port is 128.

Overview

Feature	Description
Enabling Port Security	Creates a secure address list for a port.
Filtering Layer-2 Users	Processes the packets received by a port from non-secure addresses.
Filtering Layer-3 Users	Checks the layer-2 and layer-3 addresses of packets passing a port.
Aging of Secure Addresses	Regularly deletes secure addresses.

4.3.1 Enabling Port Security

Enable port security for a port to restrict packets that access the network through the port.

Working Principle

When port security is enabled, the device security module will check the sources of received packets. Only packets from addresses in the secure address list can be normally forwarded; otherwise, the packets will be discarded or the port performs other violation handling behaviors.

When the port security and 802.1x are configured at the same time, packets can enter a switch only when the MAC addresses of the packets meet the static MAC address configurations of 802.1x or port security. If a port is configured with a secure channel or is bound to global IP+MAC, packets in compliance with the secure channel or bound to global IP+MAC can avoid checking of port security.

Related Configuration

▾ [Enabling Port Security for a Port](#)

By default, port security is disabled.

You can run the **switchport port-security** command to enable or disable the port security function for a port.

You cannot enable this function for a destination port of SPAN.

▾ [Setting the Mode for Handling Violation](#)

By default, when the number of secure addresses reaches the maximum number, the secure port will discard packets from unknown addresses (none of the secure addresses of the port).

You can run the **switchport port-security violation** command to modify the violation handling mode.

4.3.2 Filtering Layer-2 Users

Set the secure addresses on a port to ensure that only devices whose MAC addresses are the same as the secure addresses can access the network through this port.

Working Principle

Add secure addresses for a secure port. When the number of secure addresses for a secure port does not reach the maximum number, the secure port can dynamically learn new dynamic secure addresses. When the number of secure addresses for the secure port reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. The MAC addresses of users connecting to this port must be in the secure address list; otherwise, violation events will be triggered.

Related Configuration

↳ Adding Secure Addresses for a Secure port

By default, a port dynamically learns secure addresses. If an administrator has special requirements, the administrator can manually configure secure addresses.

You can run the **switch portport-security interface** command to add or delete secure addresses for a device.

4.3.3 Filtering Layer-3 Users

Add binding of secure addresses and check layer-2 and layer-3 addresses of packets passing a port.

Working Principle

Layer-3 secure addresses support only IP binding and IP+MAC binding, and supports only static binding (not dynamic binding).

When a layer-3 secure port receives packets, layer-2 and layer-3 addresses need to be parsed. Only packets whose addresses are bound are valid packets. Other packets are considered as invalid packets and will be discarded, but no violation event will be triggered.

Related Configuration

↳ Configuring Binding of Secure Addresses on Secure Ports

Binding of layer-3 secure addresses must be added manually.

You can run the **switchport port-security binding** command to add binding of secure addresses.

If only IP addresses are input, only IP addresses are bound. If IP addresses and MAC addresses are input, IP+MAC will be bound.

If only IP addresses are bound, the MAC addresses of packets are manually configured or dynamically learned. Only packets with bound IPs are allowed to enter the device.

If IP+MAC are bound, the MAC addresses of packets are manually configured or dynamically learned. Only packets with bound IP+MAC are allowed to enter the device.

4.3.4 Aging of Secure Addresses

Regularly delete secure addresses. When this function is enabled, the device can automatically add and delete secure addresses on this port based on the maximum number of secure addresses.

Working Principle

Enable the aging timer to regularly query and delete secure addresses whose aging time expires.

Related Configuration

▾ [Configuring Aging Time of Secure Addresses](#)

By default, no secure address of a port will be aged.

You can run the **switchport port-security aging** command to enable aging time.

The **static** parameter can be used to age static addresses.

4.4 Configuration

Configuration	Description and Command	
Configuring Secure ports and Violation Handling Modes	⚠ (Mandatory) It is used to enable the port security service.	
	switchport port-security	Enables port security.
	switchport port-security violation	Configures the violation handling mode for port security.
Configuring Secure Addresses on Secure Ports	⚠ (Optional) It is used to configure security filtering items.	
	switchport port-security mac-address	Configures the static secure addresses in the interface configuration mode.
	switchport port-security interface mac-address	Configures the static secure addresses in the global configuration mode.
	switchport port-security binding	Configures binding of secure addresses in the interface configuration mode.
	switchport port-security interface binding	Configures binding of secure addresses in the global configuration mode.
	switchport port-security aging	Configures aging time for all secure addresses on a port.

4.4.1 Configuring Secure ports and Violation Handling Modes

Configuration Effect

- Restrict the number of MAC addresses that can be learned from a port.
- Filter invalid packets based on MAC addresses, IP addresses or IP+MAC.

Notes

- A secure port cannot be the destination port of SPAN.
- The port security function cannot be configured for a DHCP Snooping trusted port.
- The port security function cannot be configured for excluded ports of global IP+MAC.
- The security function can be enabled only for wired switching ports and layer-2 AP ports in the interface configuration mode.
- The port security can work with other access control functions such as the 802.1x, global IP+MAC binding, and IP source guard. When these functions are used together, packets can enter a switch only when passing all security checks. If a security channel is configured for a port, packets in compliance with the security channel will avoid checking of the port security.

Configuration Steps

▾ Enabling the Port Security Service

- Mandatory.
- If there is no special requirement, enable the port security service for a port on the access device.

▾ Configuring Violation Handling Modes

- Optional. If you hope that other handling modes except discarding packets are implemented in case of violation, you can configure other handling modes.
- Configure this item on a port enabled with port security.

▾ Saving Dynamically Learned Addresses

- Optional. If you hope that secure addresses are not re-learned after the device is restarted, you can configure this item.
- Configure this item on a port enabled with port security.

Verification

Run the command of the device for displaying the port security configurations to check whether the configurations take effect.

Related Commands

▾ Setting Port Security

Command	switchport port-security
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	By using the port security feature, you can strictly control the input of a port of a device by restricting the MAC addresses and IP addresses (optional) that access the port.

↘ **Configuring the Violation Handling Mode for Port Security**

Command	switchport port-security violation { protect restrict shutdown }
Parameter Description	protect: Discards violated packets. restrict: Discards violated packets and send trap notifications. shutdown: Discards packets and disables the port.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration

Example

↘ **Enabling Port Security for the Port gigabitethernet 0/3, and Setting the Violation Handling Mode to protect**

Configuration Steps	<ul style="list-style-type: none"> ● Enable port security. ● Modify the violation handling mode.
	<pre>Ruijie# configure terminal Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security violation protect Ruijie(config-if-GigabitEthernet 0/3)# end</pre>
Verification	Check the port security configuration on the device.
	<pre>Ruijie# show port-security interface gigabitethernet 0/3 Interface : GigabitEthernet 0/3 Port status : down Port Security : enabled SecureStatic address aging : disabled Sticky dynamic address : disabled Violation mode : protect Maximum MAC Addresses : 128 Total MAC Addresses : 0 Configured MAC Addresses : 0 Dynamic MAC Addresses : 0 Sticky MAC Addresses : 0 Total security binding : 0 IPv4-ONLY Binding Addresses : 0 IPv6-ONLY Binding Addresses : 0 IPv4-MAC Binding Addresses : 0 IPv6-MAC Binding Addresses : 0 Aging time (min) : 0</pre>

Common Errors

- Port security is enabled on a SPAN port.
- Port security is enabled on a DHCP trusted port.

4.4.2 Configuring Secure Addresses on Secure Ports

Configuration Effect

- Allow specified users to use ports.
- Regularly update secure addresses of users.

Configuration Steps

▾ Configuring Secure Addresses

- Optional. You need to manually add secure addresses for configuration.
- Configure this item on a port enabled with port security.

▾ Configuring Binding of Secure Addresses

- Optional. You need to add layer-3 secure addresses for configuration.
- Configure this item on a port enabled with port security.

▾ Configuring Aging Time

- Optional.
- Configure this item on a port enabled with port security.

Verification

- Run the command of the device for displaying the port security configurations to check whether the configurations take effect.

Related Commands

▾ Adding Secure Addresses for Secure Ports in the Global Configuration Mode

Command	switchport port-security interface <i>interface-id</i> mac-address <i>mac-address</i> [vlan <i>vlan-id</i>]
Parameter Description	interface <i>interface-id</i> : Indicates the interface ID. mac-address <i>mac-address</i> : Indicates a static secure address. vlan <i>vlan-id</i> : Indicates the VID of a MAC address.
Command Mode	Global configuration mode
Usage Guide	-

▾ Adding Secure Addresses for Secure Ports in the Interface Configuration Mode

Command	switchportport-security mac-address <i>mac-address</i> [vlan <i>vlan_id</i>]
Parameter Description	mac-address <i>mac-address</i> : Indicates a static secure address. vlan <i>vlan-id</i> : Indicates the VID of a MAC address.

Command Mode	Interface configuration mode
Usage Guide	-

➤ Adding Binding of Secure Addresses for Secure Ports in the Global Configuration Mode

Command	switchport port-security interface <i>interface-id</i> binding [<i>mac-address</i> vlan <i>vlan_id</i>] <i>ipv4-address</i>
Parameter Description	interface <i>interface-id</i> : Indicates the interface ID. mac-address : Indicates a bound source MAC address. vlan <i>vlan_id</i> : Indicates the VID of a bound source MAC address. ipv4-address : Indicates a bound IPv4 address.
Command Mode	Global configuration mode
Usage Guide	-

➤ Adding Binding of Secure Addresses for Secure Ports in the Interface Configuration Mode

Command	switchport port-security binding [<i>mac-address</i> vlan <i>vlan_id</i>] <i>ipv4-address</i>
Parameter Description	mac-address : Indicates a bound source MAC address. vlan <i>vlan_id</i> : Indicates the VID of a bound source MAC address. ipv4-address : Indicates a bound IPv4 address.
Command Mode	Interface configuration mode
Usage Guide	-

➤ Configuring Aging Time for All Secure Addresses on a Port

Command	switchport port-security aging { static time <i>time</i> }
Parameter Description	static : Indicates that the aging time will be applied to manually configured secure addresses and automatically learned addresses; otherwise, the aging time will be applied to only automatically learned addresses. time <i>time</i> : Indicates the aging time of the secure addresses on this port, ranging from 0 to 1440 minutes. If it is set to 0, it indicates that the aging function is disabled actually.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration

Example

➤ Configuring a Secure MAC Address 00d0.f800.073c for the Port gigabitethernet 0/3

Configuration Steps	<ul style="list-style-type: none"> ● Enable port security. ● Add a secure address.
	<pre>Ruijie# configure terminal</pre> <p>Enter configuration commands, one per line. End with CNTL/Z.</p>

	<pre>Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security mac-address 00d0.f800.073c vlan 1 Ruijie(config-if-GigabitEthernet 0/3)# end</pre>														
Verification	Check the port security configuration on the device.														
	<pre>Ruijie# show port-security address</pre> <table border="1"> <thead> <tr> <th>NO.</th> <th>VLAN</th> <th>MacAddress</th> <th>PORT</th> <th>TYPE</th> <th>RemainingAge (mins)</th> <th>STATUS</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1</td> <td>00d0.f800.073c</td> <td>GigabitEthernet 0/3</td> <td>Configured</td> <td>--</td> <td>active</td> </tr> </tbody> </table>	NO.	VLAN	MacAddress	PORT	TYPE	RemainingAge (mins)	STATUS	1	1	00d0.f800.073c	GigabitEthernet 0/3	Configured	--	active
NO.	VLAN	MacAddress	PORT	TYPE	RemainingAge (mins)	STATUS									
1	1	00d0.f800.073c	GigabitEthernet 0/3	Configured	--	active									

📌 **Configuring a Security Binding of the IP Address 192.168.12.202 for the Port gigabitethernet 0/3**

Configuration Steps	<ul style="list-style-type: none"> ● Enable port security. ● Add a binding of the secure address. 														
	<pre>Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security binding 192.168.12.202 Ruijie(config-if-GigabitEthernet 0/3)# end</pre>														
Verification	Check the port security configuration on the device.														
	<table border="1"> <thead> <tr> <th>NO.</th> <th>VLAN</th> <th>MacAddress</th> <th>PORT</th> <th>IpAddress</th> <th>FilterType</th> <th>FilterStatus</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>--</td> <td>--</td> <td>Gi0/3</td> <td>192.168.12.202</td> <td>ipv4-only</td> <td>active</td> </tr> </tbody> </table>	NO.	VLAN	MacAddress	PORT	IpAddress	FilterType	FilterStatus	1	--	--	Gi0/3	192.168.12.202	ipv4-only	active
NO.	VLAN	MacAddress	PORT	IpAddress	FilterType	FilterStatus									
1	--	--	Gi0/3	192.168.12.202	ipv4-only	active									

📌 **Configuring the Aging Time of the Port gigabitethernet 0/3 to 8 Minutes, Which Is Also Applied to Statically Configured Secure Addresses**

Configuration Steps	<ul style="list-style-type: none"> ● Enable port security. ● Configure aging time.
	<pre>Ruijie# configure terminal Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security aging time 8</pre>

	<pre>Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security aging static Ruijie(config-if-GigabitEthernet 0/3)# end</pre>
Verification	Check the port security configuration on the device.
	<pre>Ruijie# show port-security interface gigabitethernet 0/3 Interface : GigabitEthernet 0/20 Port status : down Port Security : enabled SecureStatic address aging : enabled Sticky dynamic address : disabled Violation mode : protect Maximum MAC Addresses : 128 Total MAC Addresses : 0 Configured MAC Addresses : 0 Dynamic MAC Addresses : 0 Sticky MAC Addresses : 0 Total security binding : 0 IPv4-ONLY Binding Addresses : 0 IPv6-ONLY Binding Addresses : 0 IPv4-MAC Binding Addresses : 0 IPv6-MAC Binding Addresses : 0 Aging time (min) : 8</pre>

4.5 Monitoring

Displaying



Description	Command
Displays all secure addresses or all secure addresses of a specified port.	show port-security address [interface <i>interface-id</i>]
Displays all bindings or all bindings of a specified port.	show port-security binding [interface <i>interface-id</i>]
Displays all valid secure addresses of ports and the security binding records of the ports.	show port-security all
Displays the port security configurations of an interface.	show port-security interface <i>interface-id</i>
Displays the statistics about port security.	show port-security

5 Configuring SSH

5.1 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.

-  Currently, a device can work as an SSH server, supporting SSHv1 and SSHv2 versions. Ruijie 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-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.

5.2 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.
SSH Public Key Authentication	Use the public key authentication for SSH user authentication.

5.2.1 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 5-1 shows the network topology.

Figure 5-1 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.

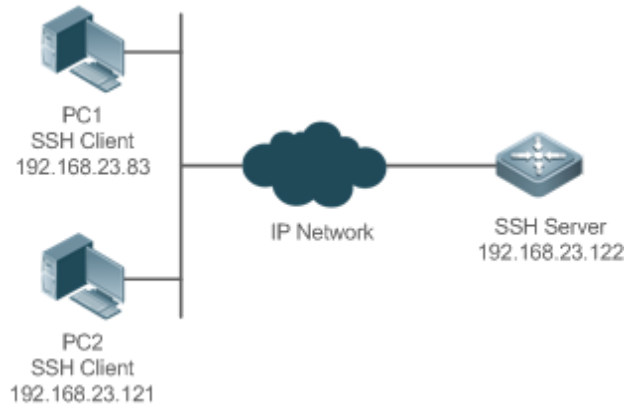
5.2.2 SSH Local Line Authentication

Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 5-2. 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 5-2 Networking Topology of SSH Local Line Password Authentication



Deployment

- Configure the SSH server as follows:
 1. Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.
 2. 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.
 3. Configure the IP address of the GigabitEthernet 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.

1. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)
2. 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".)

5.2.3 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 5-3. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 5-3 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.

5.3 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.

i 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.

5.3.1 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 or SSHv2 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 SSHv2, connecting SSHv2 clients.

By default, SSHv1 is not allowed to connect. Run the **ip ssh compatible-ssh1x enable** command to allow SSHv1 clients to connect to the server.

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 counter (CTR).

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, SHA1 is 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.

▾ Configuring Support for Diffie-Hellman(DH) Key Exchange Algorithm on the SSH Server

By default, Ruijie's SSHv2 server supports `diffie-hellman-group-exchange-sha1` and `diffie-hellman-group14-sha1` for key exchange while the SSHv1 server support none. Run the **ip ssh key-exchange** command to configure support for Diffie-Hellman on the SSH server. Use the **no ip ssh key-exchange** command to restore the default setting.

▾ Configuring Minimum Length for SSH Server Key Exchange Algorithm

The default minimum length is 2048 bytes.

Run the **ip ssh dh-exchange min-len** command to set minimum length for SSH Server key exchange algorithm. Run the **no** form of this command to restore the default settings.

▾ 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.

▾ Setting ACL Filtering of the SSH Server

By default, ACL filtering is not performed for all connections to the SSH server.


Run the **{ip | ipv6} ssh access-class** command to perform ACL filtering for all connections to the SSH server. Run **no {ip | ipv6} ssh access-class** to restore the default settings.

▾ 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.

5.4 Configuration

Configuration	Description and Command
---------------	-------------------------

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 }	Specifies the SSH message authentication algorithm.
	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.	

5.4.1 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 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.

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 SSHv2, connecting SSHv2 clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server. By default, SSHv1 clients can not connect to the 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 CTR.

↳ 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, SHA1 is supported.

▾ 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.

Verification

- Run the **show ip ssh** command to display the current SSH version, port number, encryption mode, authentication algorithm, 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

Mode	
Usage Guide	<p>The no crypto key generate command does not exist. You need to run the crypto key zeroize command to delete a key.</p> <p>SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key.</p> <p>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.</p>

↘ Specifying the SSH Version

Command	ip ssh version { 1 2 }
Parameter Description	<p>1: Indicates that the SSH server only receives the connection requests sent by SSHv1 clients.</p> <p>2: Indicates that the SSH server only receives the connection requests sent by SSHv2 clients.</p>
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 <i>time</i>
Parameter Description	<i>time</i> : 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 <i>retry times</i>
Parameter Description	<i>retry times</i> : 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 Description	<p>cbc: Sets the encryption mode supported by the SSH server to the CBC mode. Corresponding algorithms include DES-CBC,3DES-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC, and Blowfish-CBC.</p> <p>ctr: Sets the encryption mode supported by the SSH server to the CTR mode. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR.</p> <p>others: Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is</p>

	RC4.
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure the encryption mode supported by the SSH server.</p> <p>On Ruijie 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.</p> <p>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.</p>

▾ Specifying the SSH Message Authentication Algorithm

Command	<code>ip ssh hmac-algorithm { md5 md5-96 sha1 sha1-96 }</code>
Parameter Description	<p>md5: Indicates that the message authentication algorithm supported by the SSH server is MD5.</p> <p>md5-96: Indicates that the message authentication algorithm supported by the SSH server is MD5-96.</p> <p>sha1: Indicates that the message authentication algorithm supported by the SSH server is SHA1.</p> <p>sha1-96: Indicates that the message authentication algorithm supported by the SSH server is SHA1-96.</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure the message authentication algorithm supported by the SSH server.</p> <p>On Ruijie 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.</p>

▾ Configuring RSA Public Key Authentication

Command	<code>ip ssh peer test public-key rsa flash:rsa.pub</code>
Parameter Description	<p><i>test</i>: Indicates the user name.</p> <p>rsa: Indicates that the public key type is RSA.</p> <p><i>rsa.pub</i>: Indicates the name of a public key file.</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure the RSA public key file associated with user <i>test</i>.</p> <p>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.</p>

▾ Configuring DSA Public Key Authentication

Command	<code>ip ssh peer test public-key dsa flash:dsa.pub</code>
----------------	--

Parameter Description	<p><i>test</i>: Indicates the user name.</p> <p>dsa: Indicates that the public key type is DSA.</p> <p><i>dsa.pub</i>: Indicates the name of a public key file.</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure the DSA key file associated with user test.</p> <p>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.</p>

Configuration Example

 The following configuration examples describe only configurations related to SSH.

Generating a Public Key on the SSH Server

Configuration Steps	<ul style="list-style-type: none"> Run the crypto key generate { rsa dsa } command to generate a RSA public key for the server.
SSH Server	<pre>Ruijie#configure terminal Ruijie(config)# crypto key generate rsa</pre> <p>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.</p> <p>How many bits in the modulus [512]:</p> <ul style="list-style-type: none"> If the generation of the RSA key is successful, the following information is displayed: <pre>% Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok]</pre> If the generation of the RSA key fails, the following information is displayed: <pre>% Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]</pre>
Verification	<ul style="list-style-type: none"> 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	<pre> Ruijie(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 qFIKDj1j 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 8ZCa7SII EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISglfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4liQuTIL HRgtbyEYXCfaaxU= </pre>
-------------------	--

Specifying the SSH Version

Configuration Steps	<ul style="list-style-type: none"> Run the ip ssh version { 1 2 } command to set the version supported by the SSH server to SSHv2.
SSH Server	<pre> Ruijie#configure terminal Ruijie(config)#ip ssh version 2 </pre>
Verification	<ul style="list-style-type: none"> Run the show ip ssh command to display the SSH version currently supported by the SSH server.
SSH Server	<pre> Ruijie(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 </pre>

	Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled SSH dh-exchange min-len: 2048
--	--

📌 Configuring the SSH Authentication Timeout

Configuration Steps	<ul style="list-style-type: none"> Run the ip ssh time-out <i>time</i> command to set the SSH authentication timeout to 100s.
SSH Server	<pre>Ruijie#configure terminal Ruijie(config)#ip ssh time-out 100</pre>
Verification	<ul style="list-style-type: none"> Run the show ip ssh command to display the configured SSH authentication timeout.
SSH Server	<pre>Ruijie(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled SSH dh-exchange min-len: 2048</pre>

📌 Configuring the Maximum Number of SSH Authentication Retries

Configuration Steps	<ul style="list-style-type: none"> Run the ip ssh authentication-retries <i>retry times</i> command to set the maximum number of user authentication retries on the SSH server to 2.
SSH Server	<pre>Ruijie#configure terminal Ruijie(config)#ip ssh authentication-retries 2</pre>
Verification	<ul style="list-style-type: none"> Run the show ip ssh command to display the configured maximum number of authentication retries.
SSH Server	<pre>Ruijie(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22</pre>

SSH Cipher Mode:	cbc,ctr,others
SSH HMAC Algorithm:	md5-96,md5,sha1-96,sha1
Authentication timeout:	120 secs
Authentication retries:	2
SSH SCP Server:	disabled
SSH dh-exchange min-len:	2048

▾ **Specifying the SSH Encryption Mode**

Configuration Steps	<ul style="list-style-type: none"> Run the ip ssh cipher-mode {cbc ctr others} command to set the encryption mode supported by the SSH server to CTR.
SSH Server	<pre>Ruijie#configure terminal Ruijie(config)# ip ssh cipher-mode ctr</pre>
Verification	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Run the ip ssh hmac-algorithm {md5 md5-96 sha1 sha1-96} command to set the message authentication algorithm supported by the SSH server to SHA1.
SSH Server	<pre>Ruijie#configure terminal Ruijie(config)# ip ssh hmac-algorithm sha1</pre>
Verification	<ul style="list-style-type: none"> Run the show ip ssh command to display the minimum length.

▾ **Configuring the Public Key Authentication**

Configuration Steps	<ul style="list-style-type: none"> 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	<pre>Ruijie#configure terminal Ruijie(config)# ip ssh peer test public-key rsaflash:rsa.pub</pre>
Verification	<ul style="list-style-type: none"> 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**

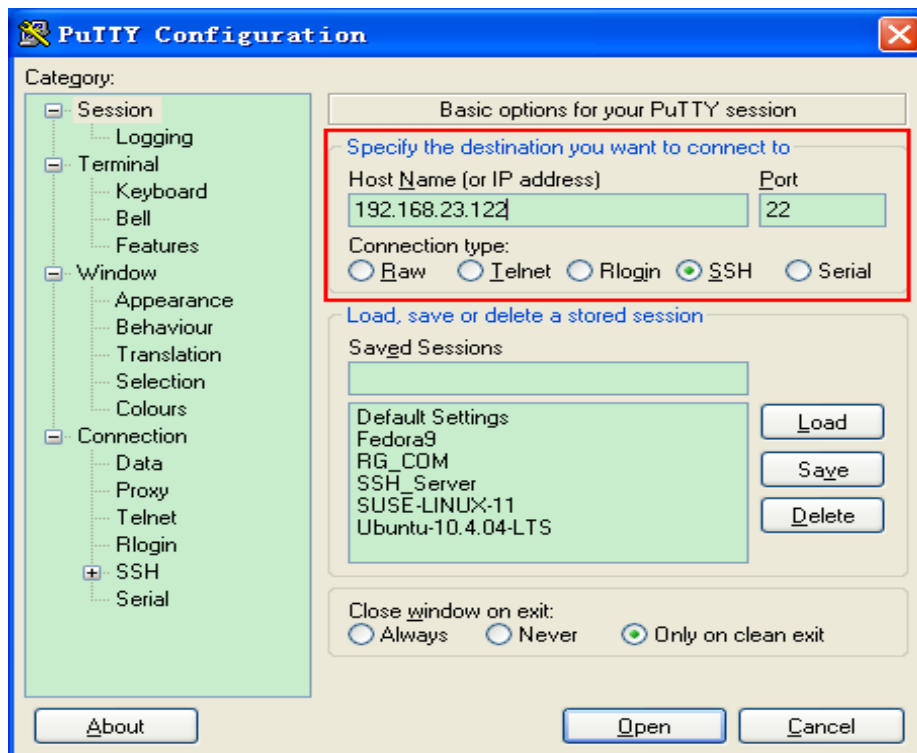
Scenario
Figure 5-4



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.

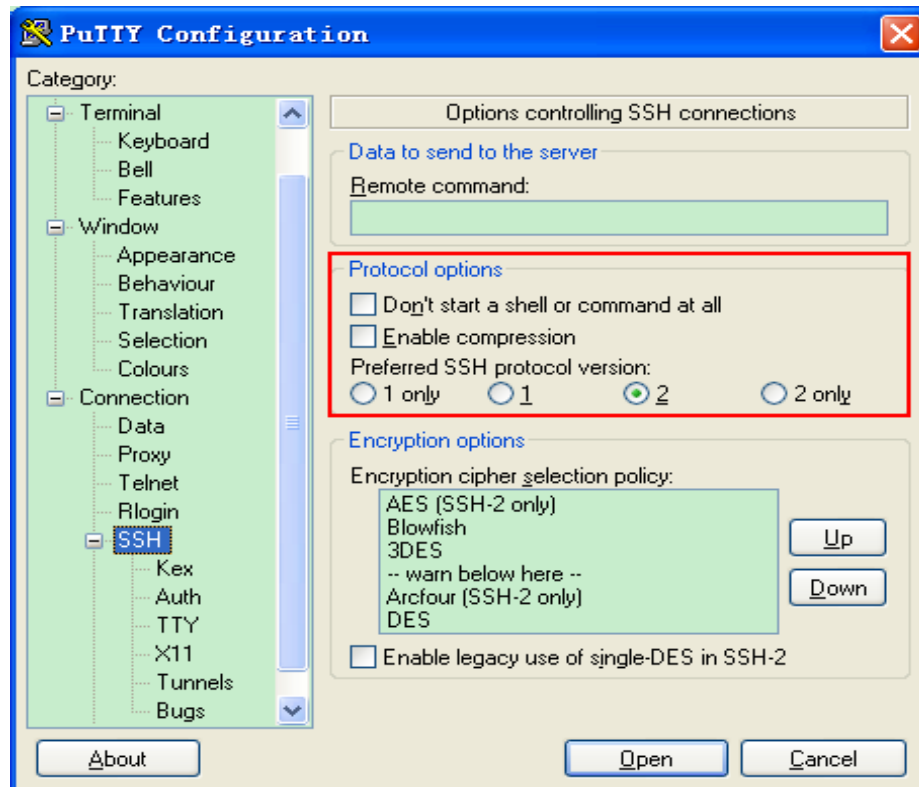
SSH Client Figure 5-5



Host Name (or IP address) indicates the IP address of the host to be logged in. In this example, the IP

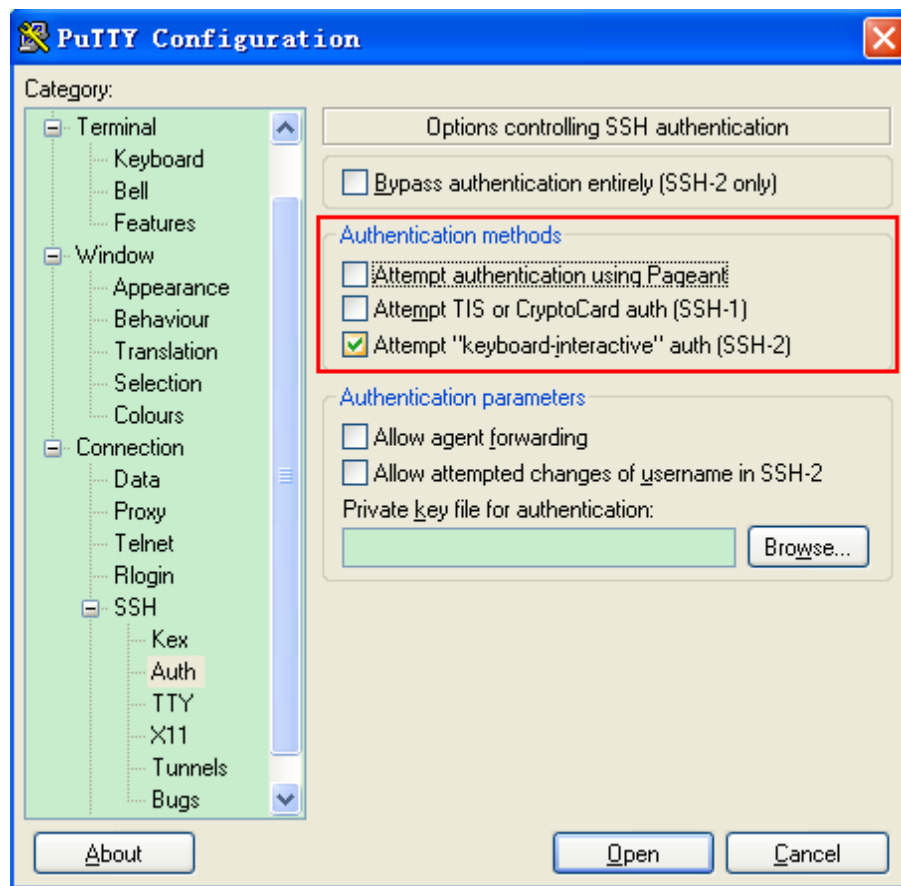
address is **192.168.23.122**. **Port** indicates the port ID 22, that is, the default ID of the port listened by SSH. **Connection type** is **SSH**.

Figure 5-6



As shown in Figure 5-6, select **2** as the preferred SSH protocol version in the **Protocol options** pane because SSHv2 is used for login.

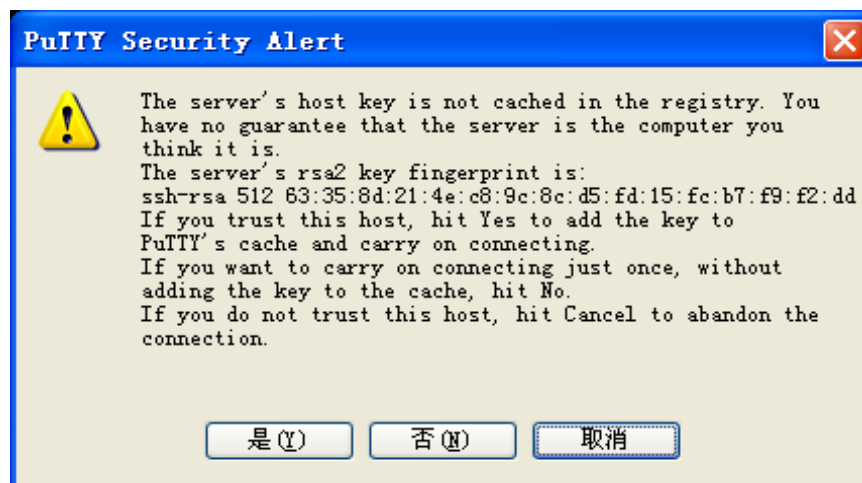
Figure 5-7



As shown in Figure 5-7, 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 5-8.

Figure 5-8



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 5-9.

Figure 5-9

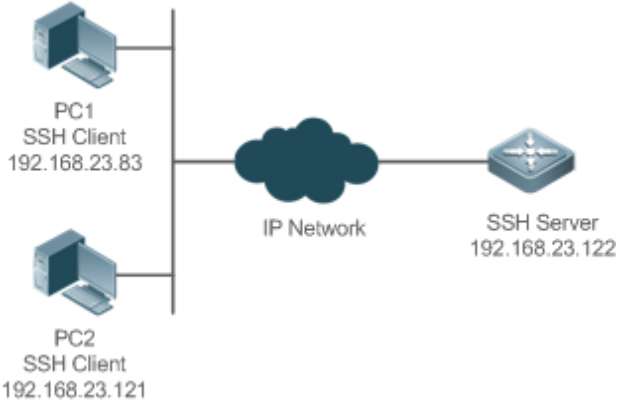


Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 5-10.

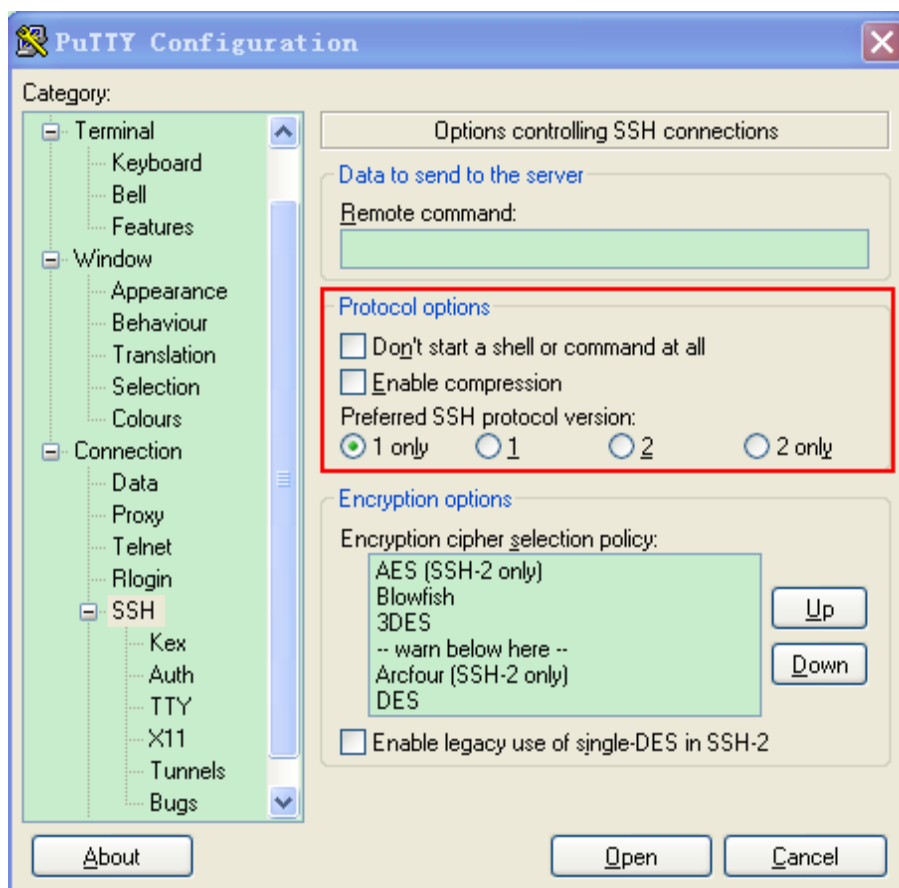
Figure 5-10

	
<p>Verification</p>	<ul style="list-style-type: none"> ● 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.
	<pre>Ruijie#show ip ssh SSH Enable - version 1.99 SSH Port: 22 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 SSH dh-exchange min-len: 2048 Ruijie#show ssh Connection Version Encryption Hmac State Username 0 2.0 aes256-cbc hmac-sha1 Session started test</pre>

➤ [Configuring SSH Local Line Authentication](#)

<p>Scenario Figure 5-11</p>	 <p>SSH users can use the local line password for user authentication, as shown in Figure 5-11. 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:</p> <ul style="list-style-type: none"> ● 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.
<p>Configuration Steps</p>	<p>Configure the SSH server as follows:</p> <ul style="list-style-type: none"> ● 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 GigabitEthernet 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. <p>Configure the SSH client as follows:</p> <ul style="list-style-type: none"> ● 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."
<p>SSH Server</p>	<p>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 5-12. The detailed procedures for configuring IP addresses and routes are omitted.</p> <pre>Ruijie(config)# enable service ssh-server Ruijie(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]:</pre>

	<p>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.</p> <p>How many bits in the modulus [512]:</p> <pre>% Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Ruijie(config)#interface vlan 1 Ruijie(config-if- VLAN 1)#ip address 192.168.23.122 255.255.255.0 Ruijie(config-if- VLAN 1)#exit Ruijie(config)#line vty 0 Ruijie(config-line)#password passzero Ruijie(config-line)#privilege level 15 Ruijie(config-line)#login Ruijie(config-line)#exit Ruijie(config)#line vty1 4 Ruijie(config-line)#password pass Ruijie(config-line)#privilege level 15 Ruijie(config-line)#login Ruijie(config-line)#exit</pre>
<p>SSH Client(PC1/PC2)</p>	<p>Figure 5-12</p>



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".)

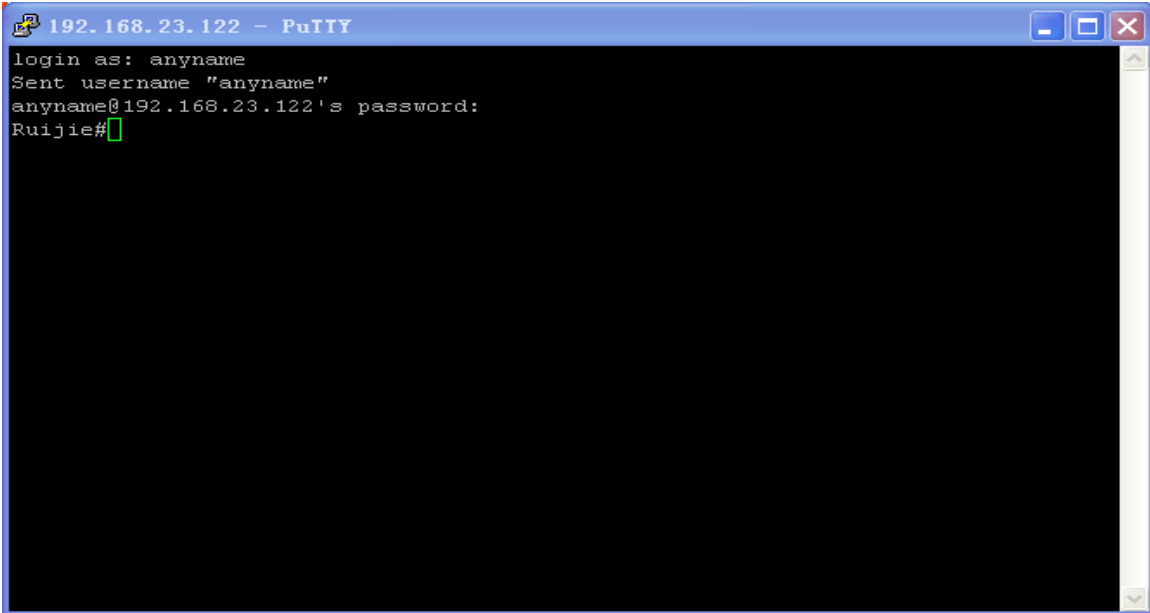
Verification

- Run the **show running-config** command to display the current configurations.
- Verify that the SSH client configurations are correct.

SSH Server


```
Ruijie#show running-config
Building configuration...

!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface VLAN 1
```

	<pre>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</pre>										
<p>SSH Client</p>	<p>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 5-13.</p> <p>Figure 5-13</p>  <pre>Ruijie#show users</pre> <table border="1"> <thead> <tr> <th>Line</th> <th>User</th> <th>Host(s)</th> <th>Idle</th> <th>Location</th> </tr> </thead> <tbody> <tr> <td>* 0 con 0</td> <td>---</td> <td>idle</td> <td>00:00:00</td> <td>---</td> </tr> </tbody> </table>	Line	User	Host(s)	Idle	Location	* 0 con 0	---	idle	00:00:00	---
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

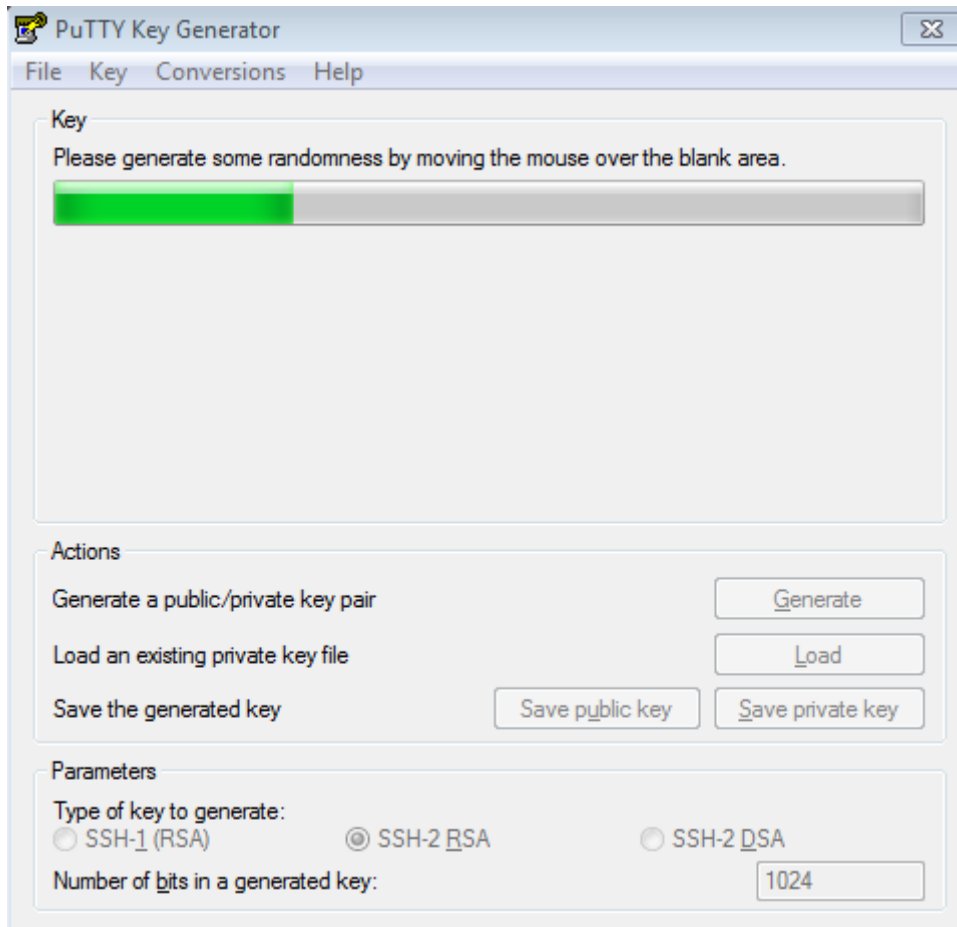
↘ **Configuring Public Key Authentication of SSH Users**

<p>Scenario Figure 5-14</p>	 <p>SSH Client 192.168.23.83</p> <p>IP Network</p> <p>SSH Server 192.168.23.122</p> <p>SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 5-14. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> 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. <p>i 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.</p> <ul style="list-style-type: none"> 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.
<p>SSH Client</p>	<p>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 5-15.</p> <p>Figure 5-15</p>



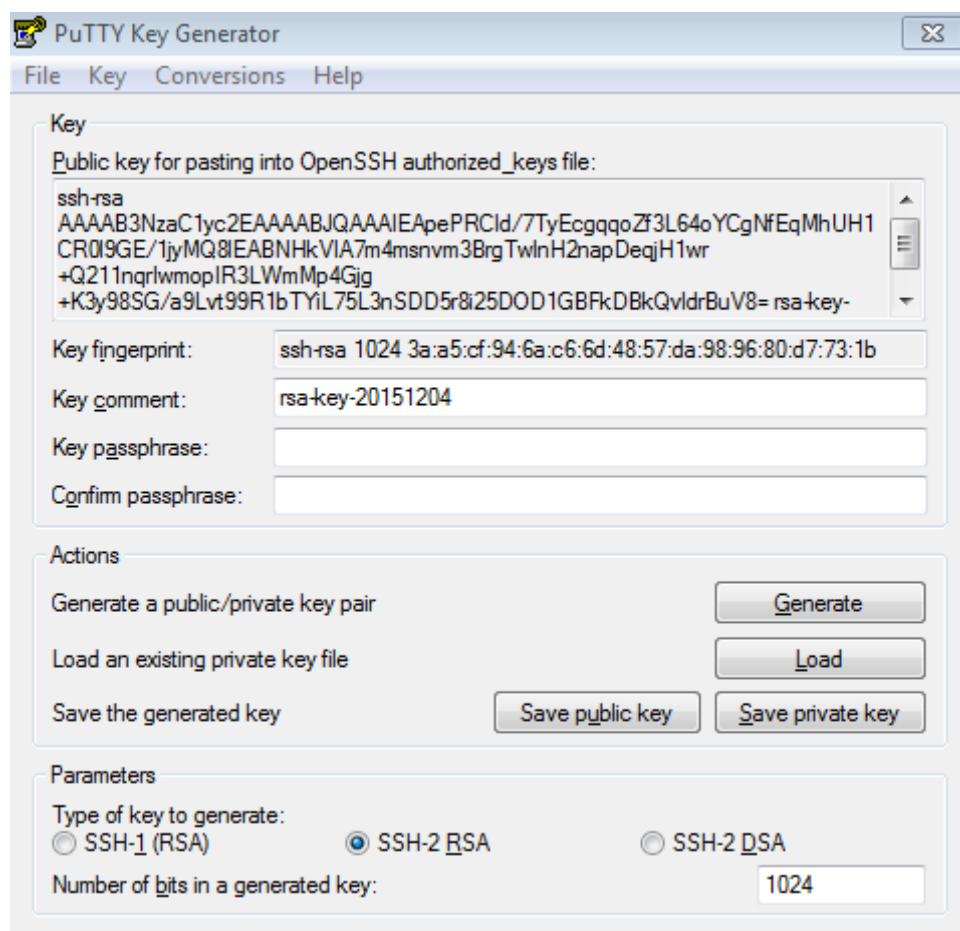
When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 5-16.

Figure 5-16



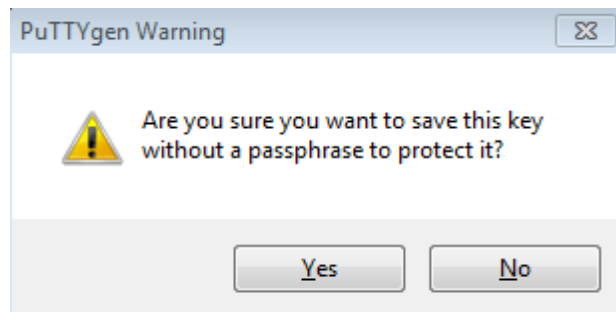
To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 5-17



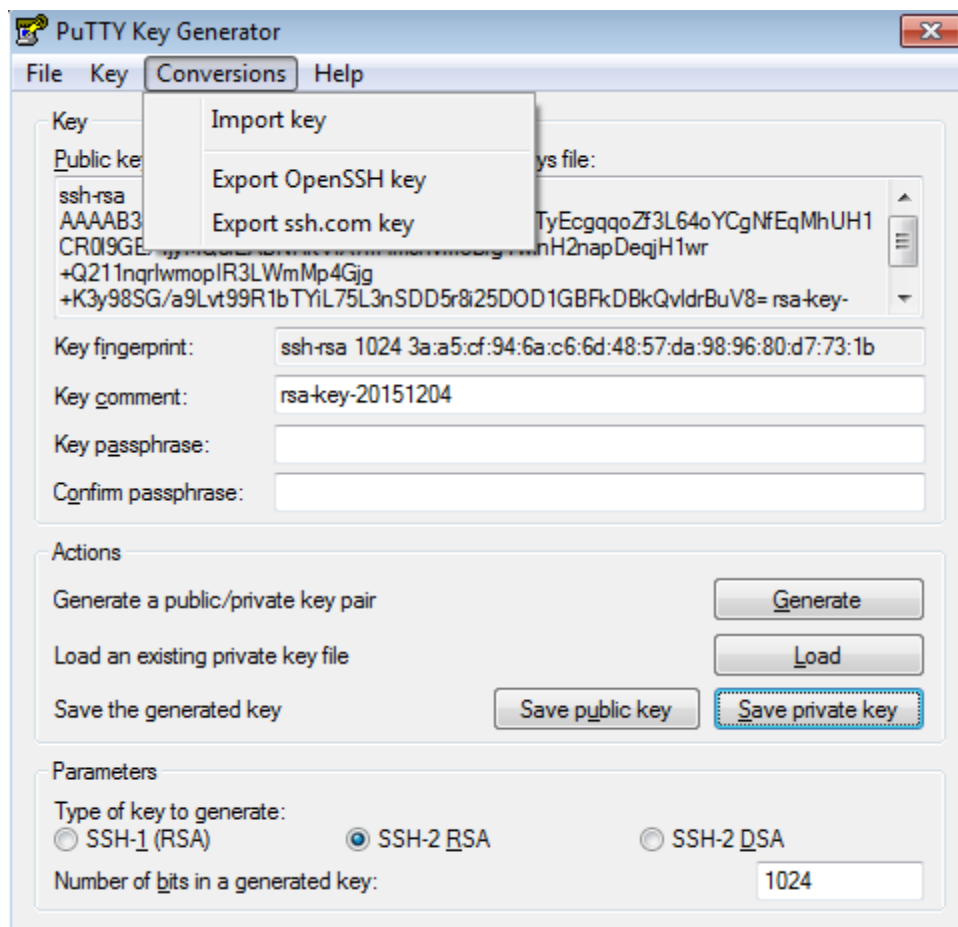
After the key pair is generated, click **Save public key**, type in the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following prompt box is displayed. Select **Yes**, type in the public key name **test_private**, and click **Save**.

Figure 5-18

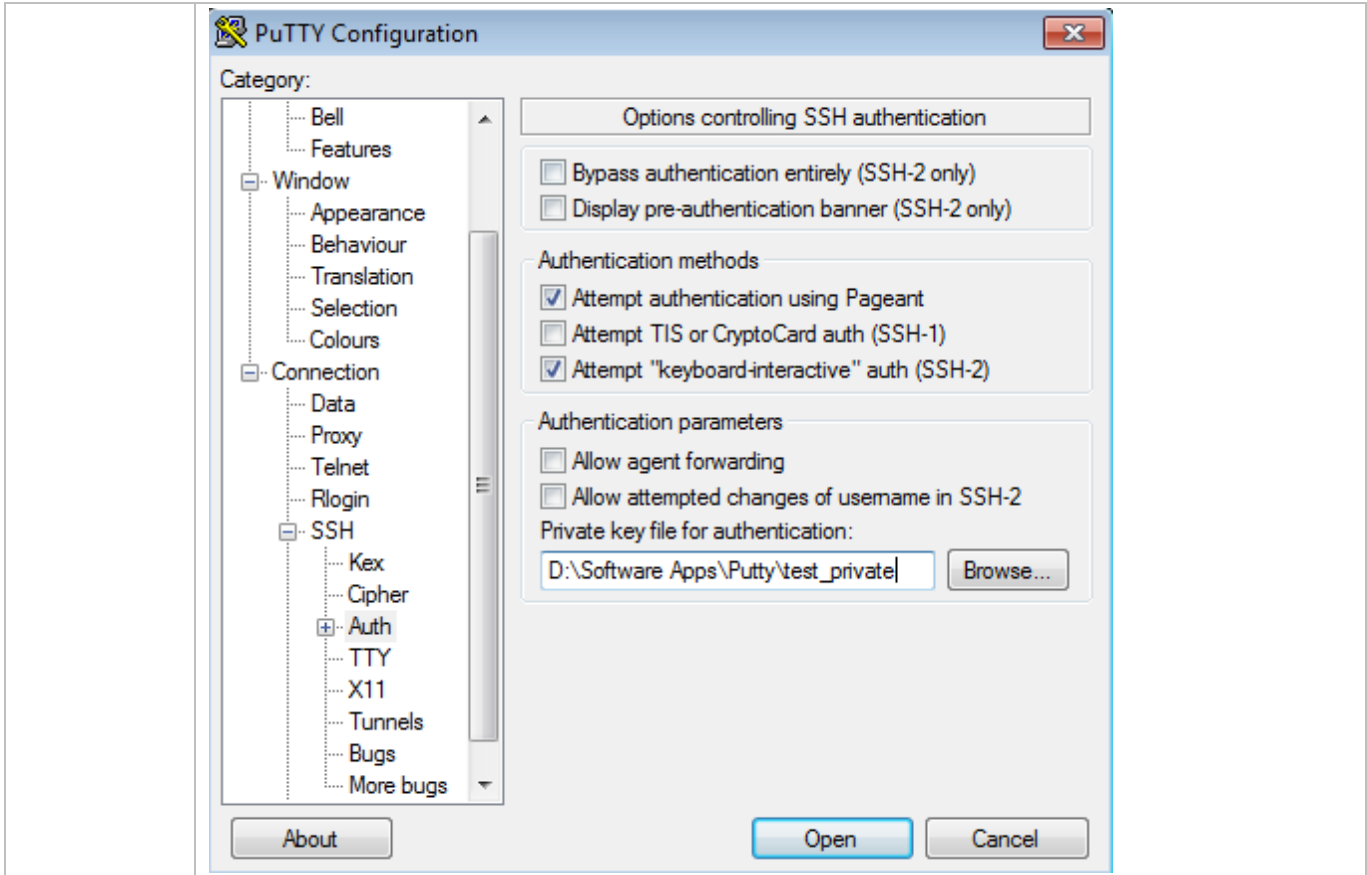


You must select the OpenSSH key file; otherwise, the key file cannot be used. The **puttygen.exe** software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. Format 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 5-19.

Figure 5-19



<p>SSH Server</p>	<pre>Ruijie#configure terminal Ruijie(config)# ip ssh peer test public-key rsaflash:test_key.pub</pre>
<p>Verification</p>	<ul style="list-style-type: none"> 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.
	<p>Figure 5-20</p>



Common Errors

- The **no crypto key generate** command is used to delete a key.

5.5 Monitoring

Displaying

Description	Command
Displays the effective SSH server configurations.	show ip ssh
Displays the established SSH connection.	show ssh
Displays the public information of the SSH public key.	show crypto key mypubkey

Debugging

 System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
-------------	---------

Debugs SSH sessions.	debug ssh
----------------------	------------------

6 Configuring CPP

6.1 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.

6.2 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.

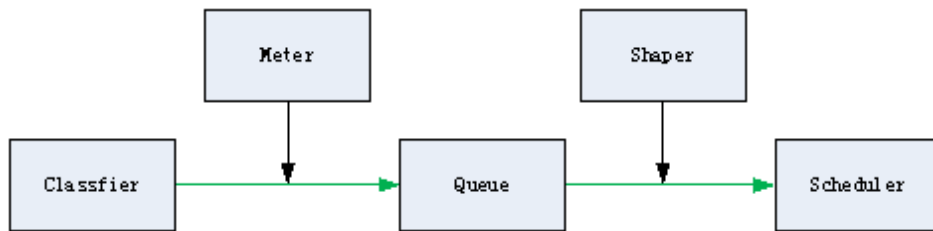
📌 **CPU interface**

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 6-1 CPP Implementation Model



Feature	Description
Classifier	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.

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 Shaper

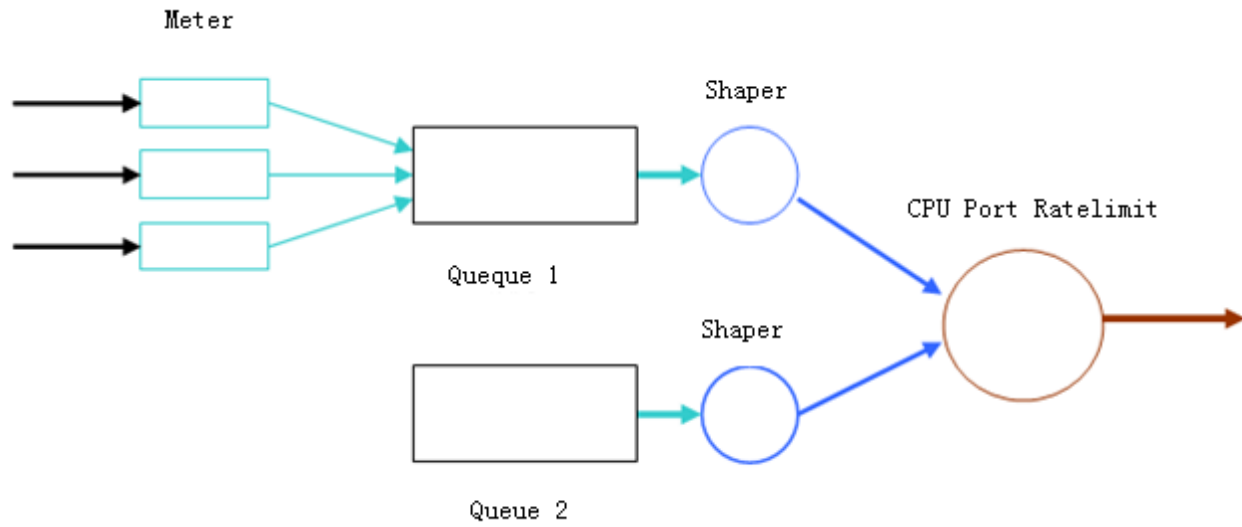
Working Principle

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 6-2 3-Level Rate Limit of the CPP



6.3 Monitoring

Clearing

Description	Command
Clears the CPP statistics.	<code>clear cpu-protect counters</code>

Displaying

Description	Command
Displays the configuration on a CPU interface.	<code>show cpu-protect</code>

7 Configuring DHCP Snooping

7.1 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.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

7.2 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.

7.2.1 Guarding Against DHCP Service Spoofing

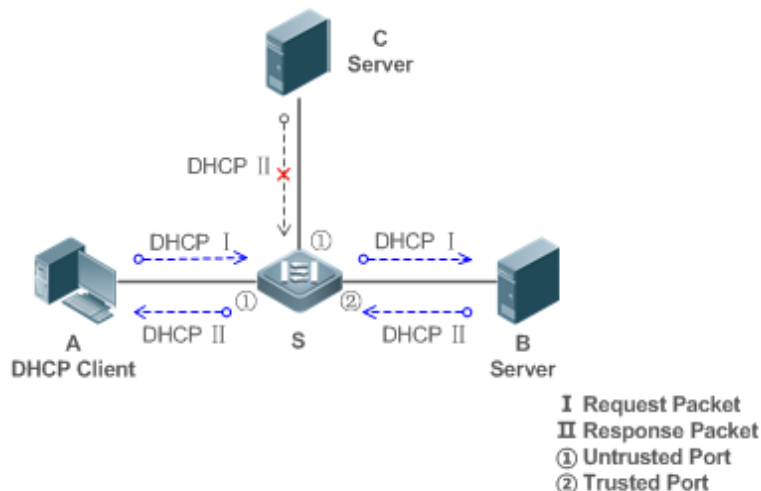
Scenario

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 7-1



Remarks:	<p>S is an access device.</p> <p>A is a user PC.</p> <p>B is a DHCP server within the controlled area.</p> <p>C is a DHCP server out of the controlled area.</p>
-----------------	--

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.

7.2.2 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.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.

7.2.3 Guarding Against Forged DHCP Packets

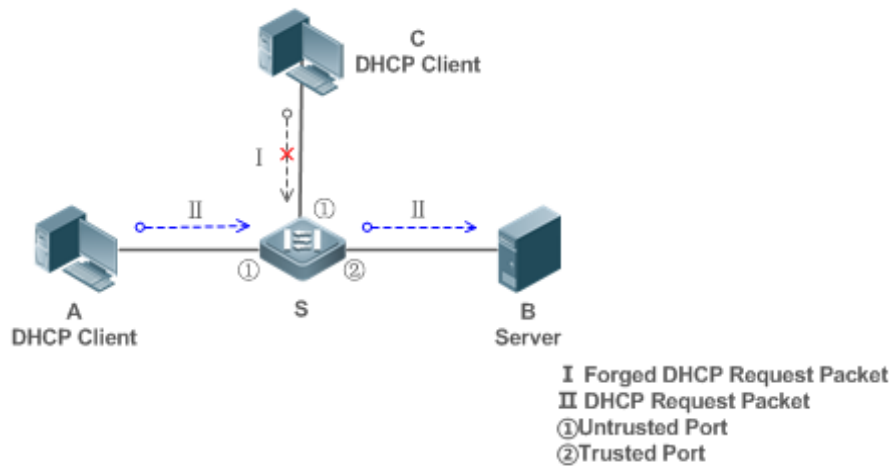
Scenario

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 7-2



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.

7.3 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.

↘ 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.

7.3.1 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 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.

7.3.2 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 (an 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.

7.4 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 vlan <i>vlan-word</i> max-user <i>user-number</i> Configures the maximum number of users bound with the VLAN.
	ip dhcp snooping suppression Enables DHCP Snooping packet suppression.
	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-bind	Enables BOOTP support.
	ip dhcp snooping check-giaddr	Enables DHCP Snooping to support the function of processing Relay requests.
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-option 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 vlan information option change-vlan-to vlan	Configures the VLAN in the circuit-id of Option82 as a specified VLAN.

7.4.1 Configuring Basic Features

Configuration Effect

- Enable DHCP Snooping.
- Configures the maximum number of users bound with the VLAN.
- 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 switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces.

Configuration Steps

▾ Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

▾ Configuring the Maximum Number of Users Bound with the VLAN

- Optional.

- 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.

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	N/A
Description	
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 the Maximum Number of Users Bound with the VLAN

Command	ip dhcp snooping vlan <i>vlan-word</i> max-user <i>user-number</i>
Parameter Description	<i>vlan-word</i> : VLAN range <i>user-number</i> : The maximum number of users bound with the VLAN, in the range from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

↘ Configuring DHCP Snooping Packet Suppression

Command	[no] ip dhcp snooping suppression
Parameter Description	N/A
Command Mode	Interface configuration 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	<i>time</i> : 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	N/A
Description	
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 Backup File Storage to the DHCP Snooping Binding Database

Command	renew ip dhcp snooping database
Parameter	N/A
Description	
Command Mode	Privileged configuration 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	N/A
Description	
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-bind
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOTP 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	<p>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.</p> <p>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.</p>

Configuration Example

DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Scenario Figure 7-3	
Configuration Steps	<ul style="list-style-type: none"> ● 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	<pre> 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 </pre>
Verification	<p>Check the configuration on Switch B.</p> <ul style="list-style-type: none"> ● 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	<pre> B#show running-config ! </pre>

```

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
NO.    MACADDRESS           IPADDRESS           LEASE(SEC)  TYPE           VLAN  INTERFACE
-----
1      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.

7.4.2 Configuring Option82

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Option82 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]
Parameter Description	standard-format: Indicates a standard 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.

➤ Configuring Sub-option remote-id of Option82 as User-defined Character String

Command	ip dhcp snooping information option format remote-id { string ASCII-string hostname } no ip dhcp snooping information option format remote-id
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	ip dhcp snooping vlan <i>vlan-id</i> information option format-type circuit-id string <i>ascii-string</i> no ip dhcp snooping vlan <i>vlan-id</i> information option
Parameter Description	<i>vlan-id:</i> Indicates the VLAN where a DHCP request packet is <i>ascii-string:</i> 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 VLAN in circuit-id of Option82 as Specified VLAN

Command	ip dhcp snooping vlan <i>vlan-id</i> information option change-vlan-to vlan <i>vlan-id</i> no ip dhcp snooping vlan <i>vlan-id</i> information option
Parameter Description	<i>vlan-id:</i> Indicates the old and new VLAN IDs
Configuration mode	Interface configuration mode
Usage Guide	Use this command to enable the option82 sub-option circuit-id and change the VLAN in the circuit-id into the specified VLAN.

Configuration Example

Configuring Option82 to DHCP Request Packets


Configuration Steps	<ul style="list-style-type: none"> Configuring basic functions of DHCP Snooping. Configuring Option82.
B	<pre>Ruijie# configure terminal Ruijie(config)# ip dhcp snooping information option Ruijie(config)# end</pre>
Verification	Check the DHCP Snooping configuration.
B	<pre>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</pre>

Common Errors

- N/A

7.5 Monitoring

Clearing


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

Description	Command
Clears dynamic user information 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 <i>H.H.H</i>
Disables debugging MAC-based DHCP Snooping.	no debug snooping ipv4 mac-address <i>H.H.H</i>
Enables debugging all DHCP Snooping	debug snooping ipv4 all
Disables debugging all DHCP Snooping	no debug snooping ipv4 all

8 Configuring ACL

8.1 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 ACLs, see the configuration manual related to QoS.

8.2 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.

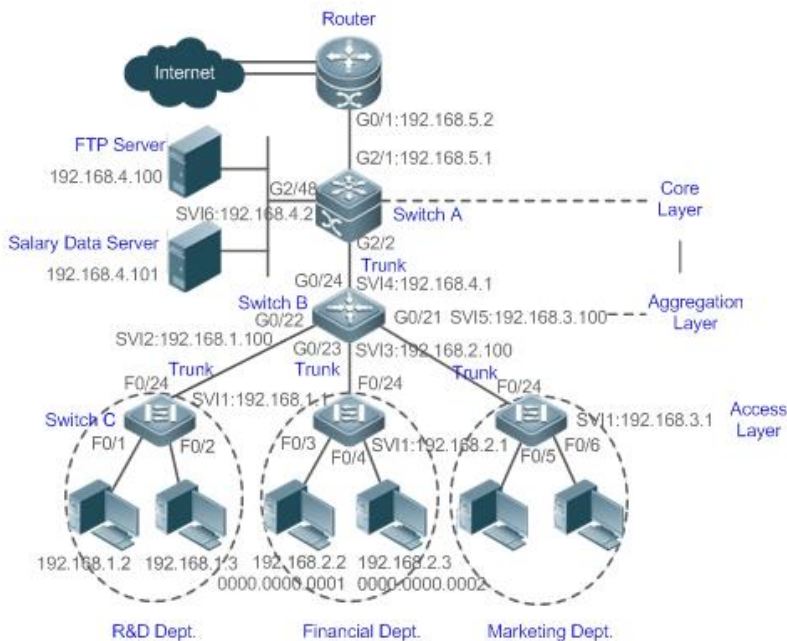
8.2.1 Access Control of an Enterprise Network

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 8-1



Remarks	<p>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).</p> <p>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).</p> <p>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.</p>
----------------	---

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.

8.3 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.

-
- i** 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 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 an interface, the device checks whether the packet matches any ACE in the input 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 used 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.

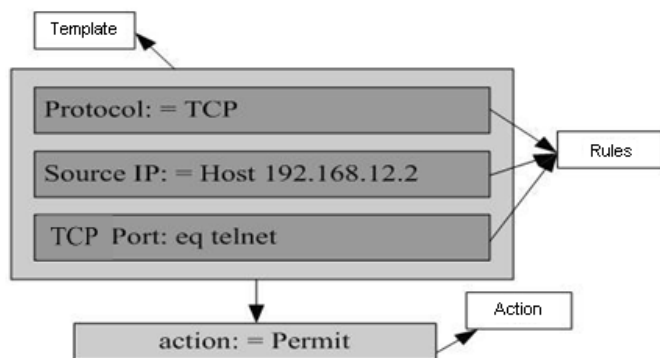
Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field 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 8-2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



Overview

Feature	Description
IP ACL	Control incoming IPv4 packets of a device based on the L3 or L4 information in the IPv4 packet header.
MAC Extended ACL	Control incoming L2 packets of a device based on the L2 information in the Ethernet packet header.

8.3.1 IP ACL

The IP ACL implements refined control on incoming 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 direction of an interface or globally. The device checks whether the incoming 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.

- ✔ For routing products, the ICMP code matching field in an ACE is ineffective for ICMP packets whose ICMP type is 3. If the ICMP code of ICMP packets to be matched is configured in an ACE, the ACL matching result of incoming ICMP packets of a device whose ICMP type is 3 may be different from the expected result.

↳ 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-id | acl-name }** 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]`
- 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 time-range-name]`

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 ] ]
```

- 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 ] ]
```

📌 Applying an IP ACL

By default, the IP ACL is not applied to any interface, that is, the IP ACL does not filter incoming 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.

8.3.2 MAC Extended ACL

The MAC extended ACL implements refined control on incoming 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 direction of an interface. The device checks whether the incoming 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 a 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 a MAC Extended ACL

By default, no MAC extended ACL is configured on a device.

Run the **mac access-list extended** { *acl-id* | *acl-name* } command in global configuration mode to create a MAC extended ACL and enter MAC extended ACL mode.

↳ Adding ACEs to a 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 a 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 ] { deny | permit } { any | host source-mac-address | source-mac-address mask } { any | host destination-mac-address | destination-mac-address mask } [ ethernet-type ] [ time-range time-range-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 { deny | permit } { any | host source-mac-address | source-mac-address mask } { any | host destination-mac-address | destination-mac-address mask } [ ethernet-type ] [ time-range time-range-name ]
```




↳ Applying a 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 L2 packets of a device.

Run the **mac access-group** { *acl-id* | *acl-name* } **in** command in interface configuration mode to apply an MAC extended ACL to a specified interface.

To collect statistics on packets with some features, run the **mac access-group** { *acl-id* | *acl-name* } **in**

8.4 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	Adds a permit ACE to a standard IP ACL.
	deny host any time-range	Adds a deny ACE to a standard IP ACL.
	permit host any host any tos dscp precedence fragment time-range	Adds a permit ACE to an extended IP ACL.
	deny host any host any tos dscp precedence fragment time-range	Adds a deny ACE to an extended IP ACL.
	ip access-group in	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 time-range	Adds a permit ACE to an MAC extended ACL.
	deny any host any host time-range	Adds a deny ACE to an MAC extended ACL.
mac access-group in	Applies an MAC extended ACL.	
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.	

8.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface to control all incoming 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 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-id acl-name }
Parameter Description	<p>standard: Indicates that a standard IP ACL is created.</p> <p>extended: Indicates that an extended IP ACL is created.</p> <p><i>acl-name:</i> 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".</p> <p><i>acl-id:</i> 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 <i>acl-id</i> is 1–99 and 1300–1999. If an extended IP ACL is created, the value range of <i>acl-id</i> is 100–199 and 2000–2699.</p>
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	[<i>sn</i>] { permit deny } { host <i>source</i> any <i>source source-wildcard</i> } [time-range <i>time-range-name</i>]
Parameter Description	<p><i>sn</i>: 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.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>host <i>source</i>: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IP packets sent from any host are filtered.</p> <p><i>source source-wildcard</i>: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>time-range <i>time-range-name</i>: 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.</p>
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 <i>acl-id</i> { permit deny } { <i>source source-wildcard</i> any host <i>source</i> } [time-range <i>time-range-name</i>]
Parameter Description	<p><i>acl-id</i>: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 100–199 and 1300–1999.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>host <i>source</i>: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>any: Indicates that IP packets sent from any host are filtered.</p> <p><i>source source-wildcard</i>: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>time-range <i>time-range-name</i>: 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.</p>
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	[<i>sn</i>] { permit deny } <i>protocol</i> { <i>source source-wildcard</i> any host source } [<i>operator port</i> [<i>port</i>]] { <i>destination destination-wildcard</i> any host destination } [<i>operator port</i> [<i>port</i>]] [[precedence precedence [tos tos]] dscp dscp] [fragment]] [time-range time-range-name]
Parameter Description	<p>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.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>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.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p>source source-wildcard: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>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.</p> <p>destination destination-wildcard: Indicates that IP packets sent to hosts in a specified IP network segment are filtered.</p> <p>any: Indicates that IP packets sent to or from any host are filtered.</p> <p>precedence precedence: Indicates that IP packets with the specified precedence field in the header are filtered.</p> <p>tos tos: Indicates that IP packets with the specified type of service (TOS) field in the header are filtered.</p> <p>dscp dscp: Indicates that IP packets with the specified dscp field in the header are filtered.</p> <p>fragment: Indicates that only fragmented IP packets except the first fragments are filtered.</p> <p>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.</p>
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 <i>acl-id</i> { deny permit } <i>protocol</i> { <i>source source-wildcard</i> any host <i>source</i> } [<i>operator port</i> [<i>port</i>]] { <i>destination destination-wildcard</i> any host <i>destination</i> } [<i>operator port</i> [<i>port</i>]] [[precedence <i>precedence</i>] [tos <i>tos</i>]] [[dscp <i>dscp</i>] [fragment] [time-range <i>time-range-name</i>]
Parameter Description	<p><i>acl-id</i>: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 100–199 and 2000–1999.</p> <p><i>sn</i>: 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.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p><i>protocol</i>: 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.</p> <p>host source: Indicates that IP packets sent from a host with the specified source IP address are filtered.</p> <p><i>source source-wildcard</i>: Indicates that IP packets sent from hosts in the specified IP network segment are filtered.</p> <p>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.</p> <p><i>destination destination-wildcard</i>: Indicates that IP packets sent to hosts in a specified IP network segment are filtered.</p> <p>any: Indicates that IP packets sent to or from any host are filtered.</p> <p><i>operator</i>: Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)</p> <p><i>port [port]</i>: Port number; <i>range</i> needs two port numbers, while other operators only need one port number.</p> <p>precedence precedence: Indicates that IP packets with the specified precedence field in the header are filtered.</p> <p>tos tos: Indicates that IP packets with the specified type of service (TOS) field in the header are filtered.</p> <p>dscp dscp: Indicates that IP packets with the specified dscp field in the header are filtered.</p> <p>fragment: Indicates that only fragmented IP packets except the first fragments are filtered.</p> <p>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.</p>
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 { <i>acl-id</i> <i>acl-name</i> } in
----------------	--

Parameter Description	<p><i>acl-id</i>: Indicates that a numbered standard or extended IP ACL will be applied to the interface.</p> <p><i>acl-name</i>: Indicates that a named standard or extended IP ACL will be applied to the interface.</p> <p><i>in</i>: Indicates that this ACL controls incoming IP packets of the interface.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>This command makes an IP ACL take effect on the incoming packets of a specified interface.</p> <p>The counter-only ACL only counts the number of matching packets and does not filter packets. In addition, the count only takes effect only to permit rules and does not take effect to deny rules in the ACL.</p>

Configuration Example

i 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 8-3	
Configuration Steps	<ul style="list-style-type: none"> ● Configure an IP ACL. ● Add ACEs to the IP ACL. ● Apply the IP ACL to the incoming direction of the interface connecting the financial data server.
SW1	<pre>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 11.1.1.0 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</pre>

Verification	<ul style="list-style-type: none"> ● 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	<pre>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</pre>

8.4.2 Configuring an MAC Extended ACL

Configuration Effect

Configure and apply an MAC extended ACL to an interface to control all incoming 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 { <i>acl-id</i> <i>acl-name</i> }
Parameter Description	<i>acl-name</i> : 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". <i>acl-id</i> : Indicates the ID that uniquely identifies an MAC extended ACL. If this option is configured, a numbered ACL is created. The value range of <i>acl-id</i> 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	[<i>sn</i>] { deny permit } { <i>source-mac-address mask</i> any host <i>source-mac-address</i> } { <i>destination-mac-address mask</i> any host <i>destination-mac-address</i> } [<i>ethernet-type</i>] [time-range <i>time-range-name</i>]
Parameter Description	<i>sn</i> : 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

	<p>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.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>any: Indicates that L2 packets sent from any host are filtered.</p> <p>host source-mac-addr: Indicates that IP packets sent from a host with the specified source MAC address are filtered.</p> <p><i>source-mac-addr mask</i>: Indicates that the source MAC address is reversed.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p>host destination-mac-addr: Indicates that IP packets sent to a host with the specified destination MAC address are filtered.</p> <p><i>destination-mac-addr mask</i>: Indicates that the destination MAC address is reversed.</p> <p><i>ethernet-type</i>: Indicates that L2 packets of the specified Ethernet type are filtered.</p> <p>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.</p>
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 <i>acl-id</i> { deny permit } { <i>source-mac-address mask</i> any host source-mac-address } { <i>destination-mac-address mask</i> any host destination-mac-address } [<i>ethernet-type</i>] [time-range time-range-name]
Parameter Description	<p><i>acl-id</i>: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of <i>acl-id</i> is 700–799.</p> <p>permit: Indicates that the ACE is a permit ACE.</p> <p>deny: Indicates that the ACE is a deny ACE.</p> <p>host source-mac-addr: Indicates that IP packets sent from a host with the specified source MAC address are filtered.</p> <p><i>source-mac-addr mask</i>: Indicates that the source MAC address is reversed.</p> <p>any: Indicates that L2 packets sent to any host are filtered.</p> <p>host destination-mac-addr: Indicates that IP packets sent to a host with the specified destination MAC address are filtered.</p> <p><i>destination-mac-addr mask</i>: Indicates that the destination MAC address is reversed.</p> <p><i>ethernet-type</i>: Indicates that L2 packets of the specified Ethernet type are filtered.</p> <p>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.</p>
Command Mode	Global configuration mode
Usage	Run this command to add ACEs to a numbered MAC extended ACL in global configuration mode. It cannot be

Guide	used to add ACEs to a named MAC extended ACL.
--------------	---

↘ **Resequencing an Extended MAC Access List**

Command	<code>mac access-list resequence { acl-id acl-name } start-sn inc-sn</code>
Parameter Description	<p><i>acl-id</i>: MAC extended access list number: 700 to 799.</p> <p><i>acl-name</i>: Name of the MAC extended access list. The name is a string of 1 to 99 characters</p> <p><i>start-sn</i>: Start sequence number. Range: 1 to 2147483647</p> <p><i>inc-sn</i>: Increment of the sequence number. Range: 1 to 2147483647</p>
Command Mode	Global configuration mode
Usage Guide	This command changes the order of the access entries.

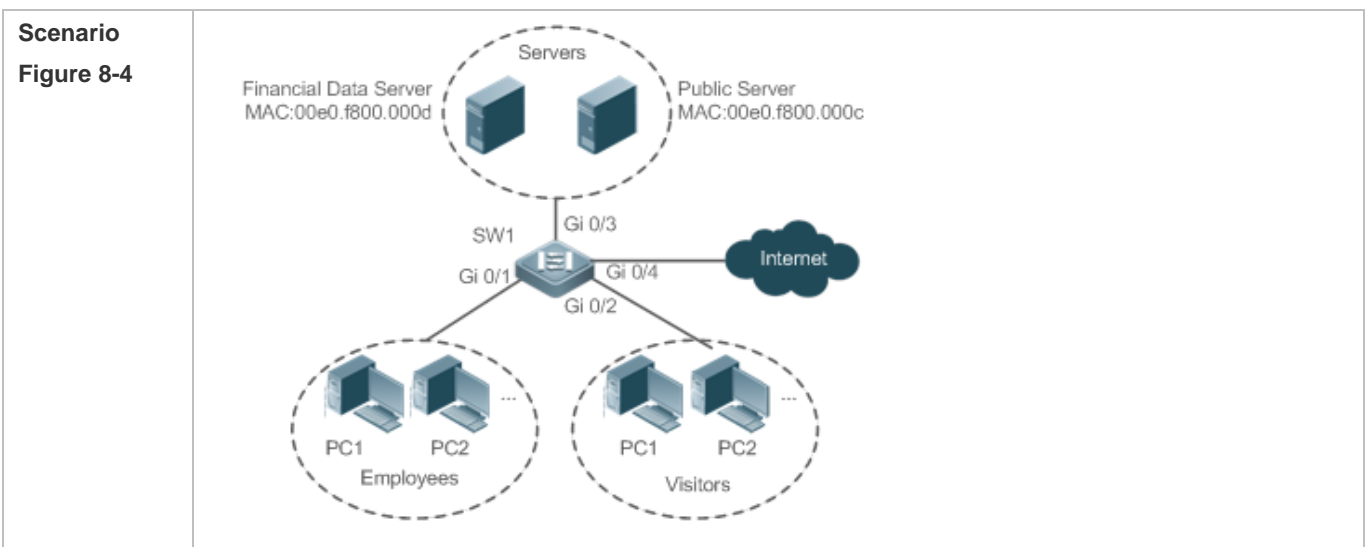
↘ **Applying an MAC Extended ACL**

Command	<code>mac access-group { acl-id acl-name } in</code>
Parameter Description	<p><i>acl-id</i>: Indicates that a numbered MAC extended IP ACL will be applied to the interface.</p> <p><i>acl-name</i>: Indicates that a named MAC extended IP ACL will be applied to the interface.</p> <p>in: Indicates that this ACL controls incoming L2 packets of the interface.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>This command makes an MAC extended ACL take effect on the incoming packets of a specified interface.</p> <p>The counter-only ACL only counts the number of matching packets and does not filter packets. In addition, the count only takes effect only to permit rules and does not take effect to deny rules in the ACL.</p>

Configuration Example

i The following configuration example describes only ACL-related configurations.

↘ **Configuring an MAC Extended ACL to Restrict Resources Accessible by Visitors**



Configuration Steps	<ul style="list-style-type: none"> ● Configure an MAC extended ACL. ● Add ACEs to the MAC extended ACL. ● Apply the MAC extended ACL to the incoming 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	<pre>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</pre>
Verification	<ul style="list-style-type: none"> ● 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	<pre>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</pre>

8.4.3 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.

▾ 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.

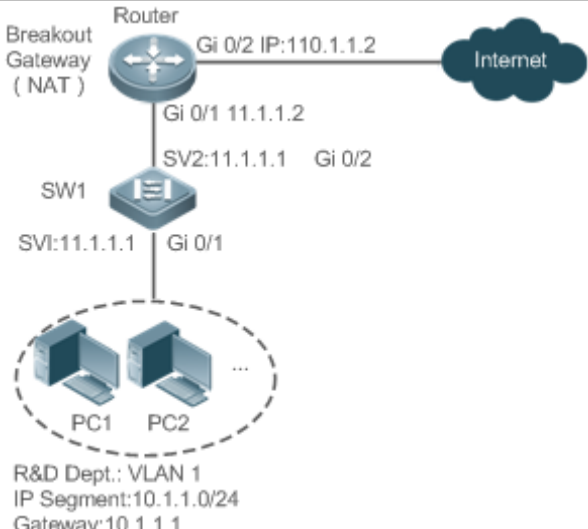
▾ Applying an ACL

For details about the command for applying an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL.

Configuration Example

i 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

<p>Scenario Figure 8-5</p>	 <p>R&D Dept.: VLAN 1 IP Segment:10.1.1.0/24 Gateway:10.1.1.1</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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 incoming direction of the interface connected to the breakout gateway.
<p>SW1</p>	<pre>sw1(config)# time-range access-internet sw1(config-time-range)# periodic daily 12:00 to 13:30 sw1(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</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● 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	<pre> 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 </pre>
------------	--

8.5 Monitoring

Displaying

Description	Command
Displays the basic ACLs.	show access-lists [<i>acl-id</i> <i>acl-ame</i>] [summary]
Displays the ACL configurations applied to an interface.	show access-group [interface <i>interface-name</i>]
Displays the IP ACL configurations applied to an interface.	show ip access-group [interface <i>interface-name</i>]
Displays the MAC extended ACL configurations applied to an interface.	show mac access-group [interface <i>interface-name</i>]

9 Configuring QoS

9.1 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.

9.2 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.

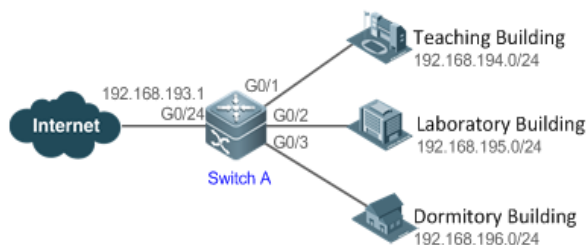
9.2.1 Interface Rate Limit + Priority Relabeling

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 9-1



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 (192.168.195.0) and laboratory (192.168.196.0) 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.

9.3 Features

Basic Concept

DiffServ

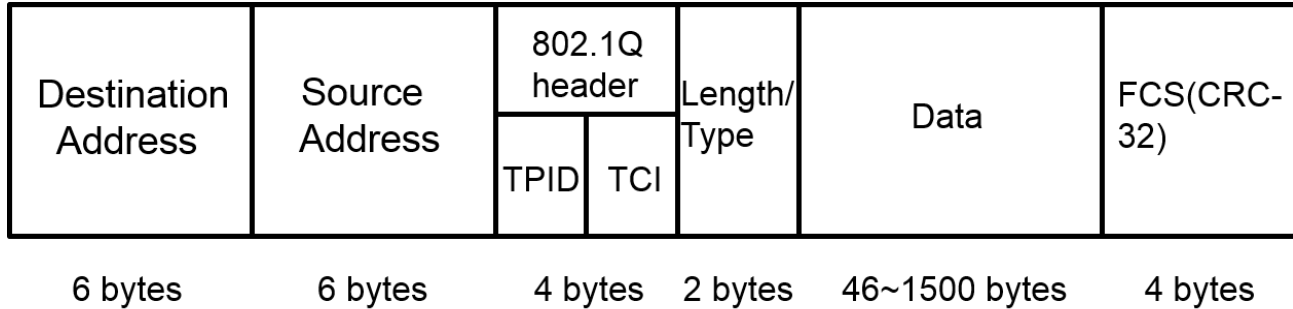
The Differentiated Services (DiffServ) Mode is an IETF system based on which QoS is implemented in Ruijie products. The DiffServ system classifies all packets transmitted in a network into different types. The classification information is included in layer-2/3 packet headers, including 802.1P, IP and 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 1-3 shows the structure of a layer-2 packet.

Figure 9-2

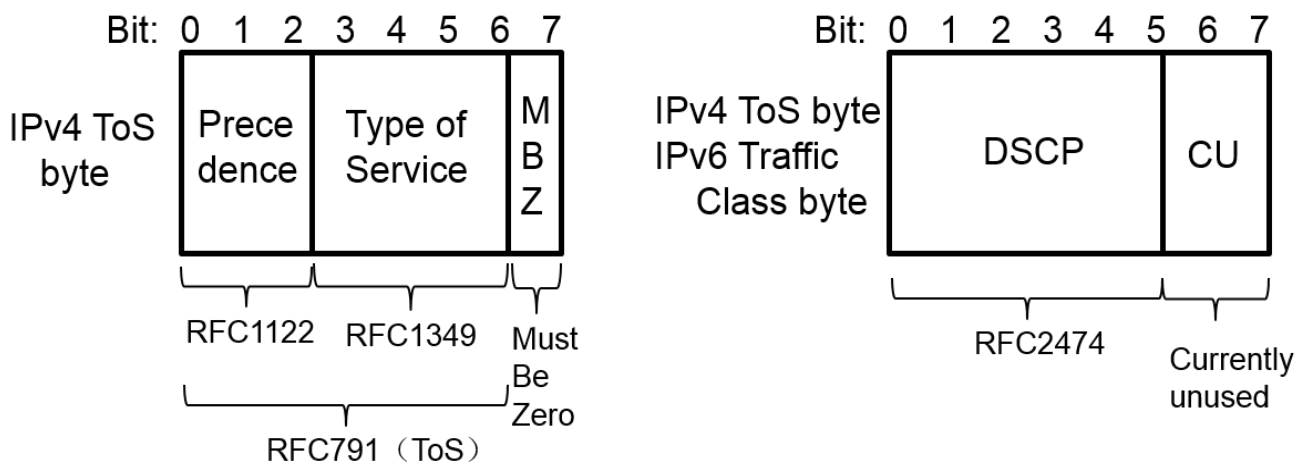


As shown in Figure 1-3, the 4-byte 802.1Q header contains 2-byte Tag Protocol Identifier (TPID) whose value is 0x8100 and 2-byte Tag Control Information (TCI). The first three bits of the TCI indicate the 802.1P priority.

➤ 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 1-4 shows the locations of the IP PRE and DSCP priorities in IPv4/IPv6 packets.

Figure 9-3



➤ CoS

Class of Service (CoS). Ruijie products convert packet priorities into CoS values to identify the local priorities of the packets and determine the input queue ID when packets are sent from the output interface.

Overview

Feature	Description
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.

9.3.1 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 have 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.

▾ 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 CoS 2, 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-precedence-dscp** command to configure the IP PRE-DSCP mapping. The DSCP value ranges from 0 to 63.

9.3.2 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 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. The traffic limit range is determined by products.

9.3.3 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 and WRR).

📌 [Scheduling policy](#)

The queue scheduling policies include SP and WRR.

- 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.

↘ 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. Some products support 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

Some products allow 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. The bandwidth limits for unicast and multicast queues are configured together on some products whereas configured separately on some other products. In addition, some products allow for configuring bandwidth only for unicast queues.

Related Configuration

↘ Configuring the scheduling policy for an output queue

By default, the scheduling policy for a global output queue is WRR and no scheduling policy is configured for an interface.

Run the **mls qos scheduler** command to configure the output scheduling policy for a queue. Configurable scheduling policies include SP and WRR.



↘ Configuring the round robin weight corresponding to the WRR scheduling policy for an output queue

By default, the weight of a global or interface-based queue is 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. The configurable weight range is determined by products.

A higher weight means longer output time.

9.4 Configuration

Configuration	Description and Command	
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.	
	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.	
	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.

9.4.1 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 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	<i>default-cos</i> : 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	<i>dscp1...dscp8</i> : 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	<i>dscp-list</i> : 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. <i>cos</i> : 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-precedence-dscp <i>dscp1...dscp8</i>
Parameter Description	<i>dscp1...dscp8</i> : 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	<ul style="list-style-type: none"> ● Modify the trust mode of the interface gigabitEthernet 0/1 to DSCP. ● Change the default CoS value of the interface gigabitEthernet 0/2 to 7.
	<pre>Ruijie# configure terminal Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# mls qos trust dscp Ruijie(config-if-GigabitEthernet 0/1)# exit Ruijie(config)# interface gigabitEthernet 0/2 Ruijie(config-if-GigabitEthernet 0/2)# mls qos cos 7 Ruijie(config-if-GigabitEthernet 0/2)# exit</pre>
Verification	NA

↘ Configuring the CoS-to-DSCP, DSCP-to-CoS, and IP-PRE-to-DSCP mappings

Configuration Steps	<ul style="list-style-type: none"> ● 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.
	<pre>Ruijie# configure terminal Ruijie(config)# mls qos map cos-dscp 7 14 21 28 35 42 49 56</pre>
	<pre>Ruijie(config)# mls qos map dscp-cos 0 1 2 3 4 to 4 Ruijie(config)# mls qos map dscp-cos 11 12 13 14 to 7</pre>

	<pre>Ruijie(config)# mls qos map ip-precedence-dscp 31 26 21 15 19 45 47 61</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Check whether all mappings are successfully configured.
	<pre>Ruijie# show mls qos maps cos-dscp cos dscp ---- ---- 0 7 1 14 2 21 3 28 4 35 5 42 6 49 7 56</pre>
	<pre>Ruijie# 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</pre>

	56	7	57	7	58	7	59	7
	60	7	61	7	62	7	63	7
<pre> Ruijie# 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 </pre>								

9.4.2 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	input: Indicates the input direction of the interface.
Description	output: Indicates the output direction of the interface.

	<i>bps</i> : Indicates the bandwidth limit per second (Kbits). The value range is determined by products. <i>burst-size</i> : Indicates the burst traffic limit (Kbytes). The value range is determined by products.
Command Mode	Interface configuration mode
Usage Guide	-

9.4.3 Configuring Congestion Management

Configuration Effect

- Configure the scheduling policy and the WRR weight for an output queue

Notes

- Interface configurations allow for only AP and Ethernet interface configurations.

Configuration Steps

↘ Configuring the scheduling policy for an output queue

- Optional.

↘ Configuring the WRR weight for an output queue

- Optional.

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.

Related Commands

↘ Configuring the scheduling policy for an output queue

Command	mls qos scheduler { sp wrr }
Parameter Description	sp : Sets the scheduling algorithm for an output queue to SP. wrr : Sets the scheduling algorithm for an output queue to WRR.
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	-

↘ Configuring the WRR weight for an output queue

Command	wrr-queue bandwidth weight1 ... weight8
Parameter	<i>weight1...weight8</i> : 8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1.

Description	For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15.
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	-

9.5 Monitoring

Displaying

Description	Command
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 <i>interface-id</i>]
Displays the QoS queue, scheduling policy and round robin weight information.	show mls qos queueing [interface <i>interface-id</i>]
Displays the scheduling information of an output queue.	show mls qos scheduler [interface <i>interface-id</i>]

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

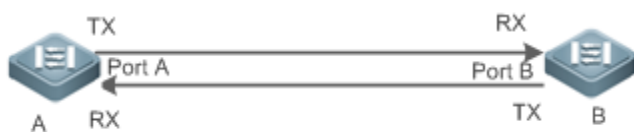
Application	Description
Unidirectional Link Detection	Detect a unidirectional link failure.
Bidirectional Forwarding Detection	Detect a bidirectional link failure.
Downlink Loop Detection	Detect a link loop.

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 1-1



Remarks	<p>A and B are layer-2 or layer-3 switches.</p> <p>The Tx of Port A of A is connected to the Rx of Port B of B.</p> <p>The Rx of Port A of A is connected to the Tx of Port B of B.</p>
----------------	---

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 1-2



Remark	A and B are layer-2 or layer-3 switches.
s	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

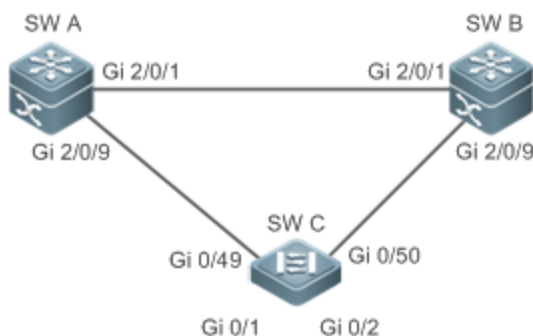
- Global RLDP is enabled.
- Configure BFD under Port A and Port B and define a method for failure treatment.

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 1-3



Remark	A, B and C are layer-2 or layer-3 switches.
s	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 neighbor negotiation, the **rldp detect-interval** to specify a detection interval, the **rldp detect-max** to specify detection times, or the **rldp reset** to recover a failed port.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic RLDP Functions	 (Mandatory) It is used to enable RLDP detection under global configuration mode.	
	rldp enable	Enables global RLDP detection on all ports.
	 (Mandatory) It is used to specify under interface configuration mode a detection type 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 under 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	
 (Optional) It is used under privileged mode.		
	rldp reset	Recovers all ports.

1.4.1 Configuring Basic RLDP Functions

Configuration Effect

- Enable RLDP unidirectional link detection, bidirectional forwarding detection, or downlink loop detection to discover 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*.

Configuration Steps

▾ Enabling RLDP

- Mandatory.
- Enable RLDP detection on all ports under global configuration mode.

▾ Enabling Neighbor Negotiation

- Optional.
- Enable the function under global configuration mode, and port detection will be started under successful neighbor negotiation.

▾ Configuring Detection Interval

- Optional.
- Specify a detection interval under global configuration mode.

↘ **Configuring Maximum Detection Times**

- Optional.
- Specify the maximum detection times under global configuration mode.

↘ **Configuring Detection under Port**

- Mandatory.
- Configure unidirectional RLDP detection, bidirectional RLDP detection or downlink loop detection under interface configuration mode, and specify failure treatment.

↘ **Restoring All Failed Ports**

- Optional.
- Enable this function under 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	<code>rldp enable</code>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable global RLDP detection.

↘ **Enabling RLDP Detection on Interface**

Command	<code>rldp port { unidirection-detect bidirection-detect loop-detect } { warning shutdown-port block }</code>
Parameter Description	<p>unidirection-detect: Indicates unidirectional link detection.</p> <p>bidirection-detect: Indicates bidirectional forwarding detection.</p> <p>loop-detect: Indicates downlink loop detection.</p> <p>warning: Indicate the failure treatment is warning.</p> <p>shutdown-port: Indicates the failure treatment is port violation.</p> <p>block: Indicates the failure treatment is disabling learning and forwarding of a port.</p>
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 <i>interval</i> detect-max <i>num</i> neighbor-negotiation }
Parameter Description	detect-interval <i>interval</i> : Indicates a detection interval. detect-max <i>num</i> : 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 <i>interface-id</i>]
Parameter Description	<i>interface-id</i> : 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 1-4	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.
--------------------------------------	---

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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.
<p>A</p>	<pre>A# configure terminal A(config)# rldp enable A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# rldp port unidirection-detect shutdown-port A(config-if-GigabitEthernet 0/1)# rldp port bidirection-detect shutdown-port A(config-if-GigabitEthernet 0/1)# exit A(config)#interface GigabitEthernet 0/9 A(config-if-GigabitEthernet 0/9)# rldp port unidirection-detect shutdown-port A(config-if-GigabitEthernet 0/9)# rldp port bidirection-detect shutdown-port A(config-if-GigabitEthernet 0/9)# rldp port loop-detect shutdown-port A(config-if-GigabitEthernet 0/9)# exit</pre>
<p>B</p>	<p>Apply the configuration on SW A.</p>
<p>C</p>	<pre>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</pre>

	<pre> 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 </pre>
Verification	<ul style="list-style-type: none"> ● Check the RLDP information on SW A, SW B and SW C. Take SW A for example.
A	<pre> A# show rldp rldp state : enable rldp hello interval: 3 rldp max hello : 2 rldp local bridge : 00d0.f822.33aa ----- Interface GigabitEthernet 0/1 port state : normal neighbor bridge : 00d0.f800.51b1 neighbor port : GigabitEthernet 0/1 unidirection detect information: action: shutdown-port state : normal bidirection detect information: action: shutdown-port state : normal Interface GigabitEthernet 0/9 port state : normal neighbor bridge : 00d0.f800.41b0 neighbor port : GigabitEthernet 0/49 unidirection detect information: action: shutdown-port state : normal </pre>


```

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.

1.5 Monitoring

Displaying

Description	Command
Displays RLDP state.	show rldp [interface <i>interface-name</i>]

Network Management & Monitoring Configuration

1. Configuring SNMP
2. Configuring NTP
3. Configuring SPAN and RSPAN

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 station, 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.

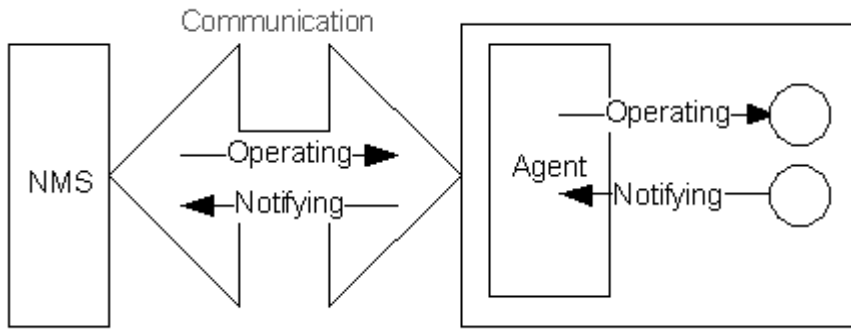
1.3 Features

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.

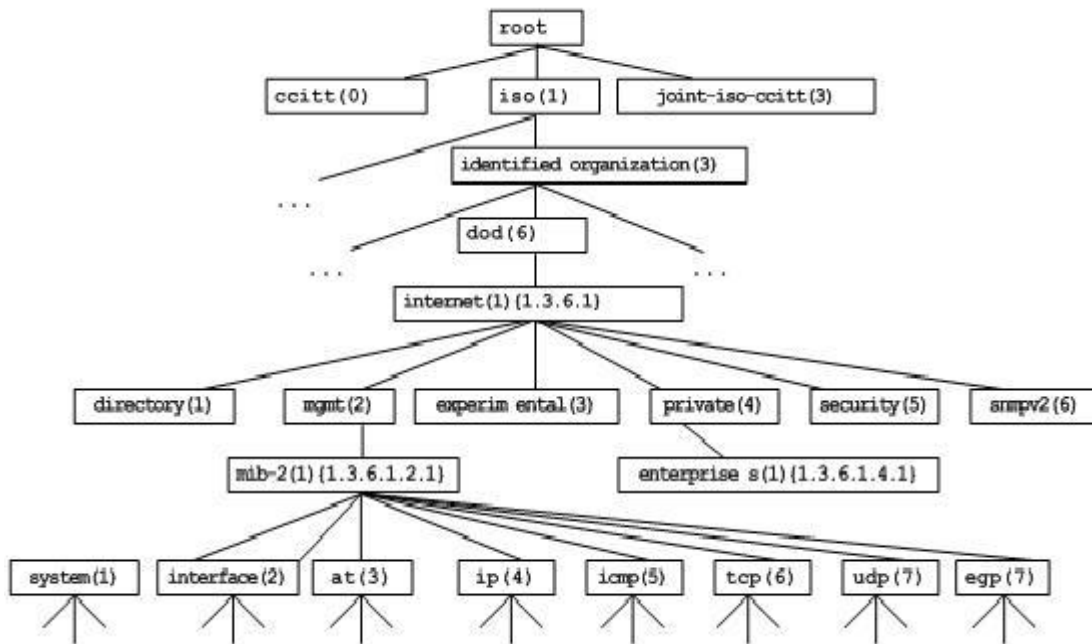
↳ **SNMP Agent**

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



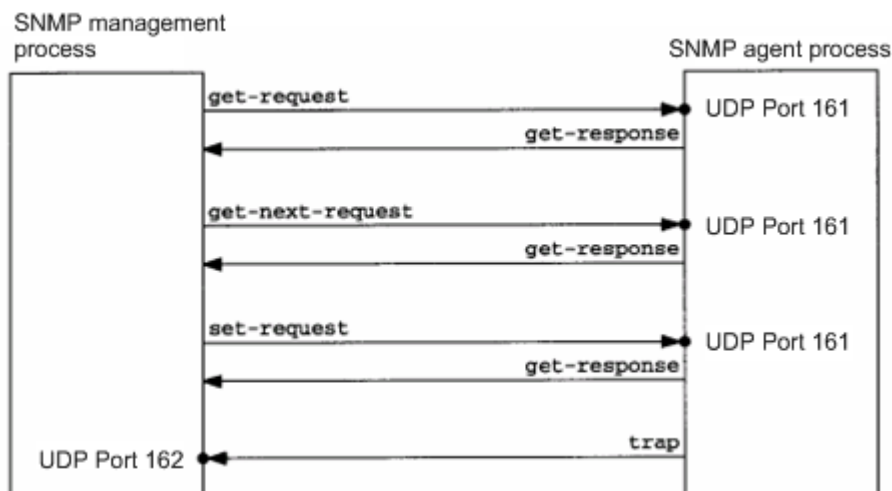
Operation Types

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 is 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 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.

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 system-shutdown** command is used to enable or disable the function of sending a system reboot trap message.

▾ Setting Password Dictionary Check for Communities and Users

By default, password dictionary check for communities and users is disabled.

The **snmp-server enable secret-dictionary-check** command is used to enable password dictionary check for SNMP communities and users. This command is used with the **password policy** command.

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 have a unique engine ID, that is, `SnmEngineID`.

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.
- 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.

1.4 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 enable secret-dictionary-check	Configures password dictionary check for communities and users.
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.
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 chassis-id	Sets the serial number of 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.

Configuration	Description and Command	
	<code>snmp-server trap-timeout</code>	Modifies the interval for sending a trap message.

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.

Setting Password Dictionary Check for Communities and Users

- Optional
- By default, password dictionary check is not performed for communities and users. If community names and user names are too simple and are easily cracked, enable password dictionary check for communities and users. The configuration must be used with the **password policy** command.

Verification

Run the **show snmp** command to check the SNMP function on devices.

Related Commands

Configuring an SNMP View

Command	snmp-server view <i>view-name oid-tree</i> { include exclude }
Parameter Description	<i>view-name</i> : View name <i>oid-tree</i> : 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 <i>groupname</i> { v1 v2c v3 { auth noauth priv } } [read <i>readview</i>] [write <i>writeview</i>] [access { <i>aclnum</i> <i>aclname</i> }]
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. <i>readview</i> : Associates one read-only view. <i>writeview</i> : Associates one read/write view. <i>aclnum</i> : ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified.

	<i>aclname</i> : ACL name. The specified ACL is associated and the range of IPv4 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] <i>string</i> [view <i>view-name</i>] [[ro rw] [host <i>ipaddr</i>]] [<i>aclnum</i> <i>aclname</i>]
Parameter Description	<p>0: Indicates that the input community string is a plaintext string.</p> <p>7: Indicates that the input community string is a ciphertext string.</p> <p><i>string</i>: Community string, which is equivalent to the communication password between the NMS and the SNMP agent.</p> <p><i>view-name</i>: Specifies a view name for view-based management.</p> <p>ro: Indicates that the NMS can only read variables of the MIB.</p> <p>rw: The NMS can read and write variables of the MIB.</p> <p><i>aclnum</i>: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified.</p> <p><i>aclname</i>: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified.</p> <p><i>ipaddr</i>: Associates NMS addresses and specifies NMS addresses for accessing the MIB.</p>
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>To disable the SNMP agent function, run the no snmp-server command.</p>

↘ **Configuring an SNMP User**

Command	snmp-server user <i>username</i> <i>groupname</i> { v1 v2c v3 [encrypted] [auth { md5 sha } <i>auth-password</i>] [priv des56 <i>priv-password</i>] } [access { <i>aclnum</i> <i>aclname</i> }]
Parameter Description	<p><i>username</i>: User name.</p> <p><i>groupname</i>: Specifies the group name for a user.</p> <p>v1 v2c v3: Specifies the SNMP version. Only SNMPv3 supports later security parameters.</p> <p>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</p>

	<p>characters stand for one byte. Encrypted keys are valid for this engine only.</p> <p>auth: Specifies whether authentication is used.</p> <p>md5: Specifies the MD5 authentication protocol. sha specifies the SHA authentication protocol.</p> <p><i>auth-password:</i> Configures a password string (not more than 32 characters) used by the authentication protocol. The system converts the passwords into the corresponding authentication keys.</p> <p>priv: Specifies whether confidentiality is used. des56 specifies the use of the 56-bit DES encryption protocol.</p> <p><i>priv-password:</i> Configures a password string (not more than 32 characters) used for encryption. The system converts the password into the corresponding encryption key.</p> <p><i>aclnum:</i> ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified.</p> <p><i>aclname:</i> ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified.</p>
Command Mode	Global configuration mode
Usage Guide	<p>Configure user information so that the NMS can communicate with the agent by using a valid user.</p> <p>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.</p>

↘ **Enabling the Agent Function**

Command	enable service snmp-agent
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command is used to enable the SNMP agent function of a device.

↘ **Setting Password Dictionary Check for Communities and Users**

Command	snmp-server enable secret-dictionary-check
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	<p>This command must be used with the password policy command to set check rules, for example, the password must consist of not less than six characters.</p> <p>To disable password dictionary check, run the no snmp-server enable secret-dictionary-check command.</p>

➤ **Displaying the SNMP Status Information**

Command	show snmp [mib user view group host process-mib-time]
Parameter Description	<p>mib: Displays information about the SNMP MIB supported in the system.</p> <p>user: Displays information about an SNMP user.</p> <p>view: Displays information about an SNMP view.</p> <p>group: Displays information about an SNMP user group.</p> <p>host: Displays information about user configuration.</p> <p>process-mib-time: Displays the MIB node with the longest processing time.</p>
Configuration mode	Privileged mode.
Usage Guide	N/A

Configuration Example

➤ **Configuring SNMPv3 Configuration (Specified View)**

<p>Scenario Figure 1-5</p>	<div style="text-align: center;"> <p>The diagram illustrates a network connection between an Agent and an NMS. The Agent is represented by a blue square icon with a crosshair, and the NMS is represented by a blue server rack icon. They are connected by a horizontal line labeled 'VLAN 1'. Below the Agent icon is the text 'IP:192.168.3.1/24', and below the NMS icon is the text 'IP:192.168.3.2/24'.</p> </div> <ul style="list-style-type: none"> ● 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.
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● 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

	<p>“DES56”, and encryption password to “321”.</p> <ul style="list-style-type: none"> ● 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 SVI 1 interface to 192.168.3.1/24.
<p>Agent</p>	<pre>Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2 Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 Ruijie(config)#snmp-server enable traps Ruijie(config)#interface vlan 1 Ruijie(config-if-VLAN 1)#ip address 192.168.3.1 255.255.255.0 Ruijie(config-if-VLAN 1)#exit</pre>
<p>Verification</p>	<ol style="list-style-type: none"> 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.
<p>Agent</p>	<pre>Ruijie# show running-config ! interface VLAN 1 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</pre>

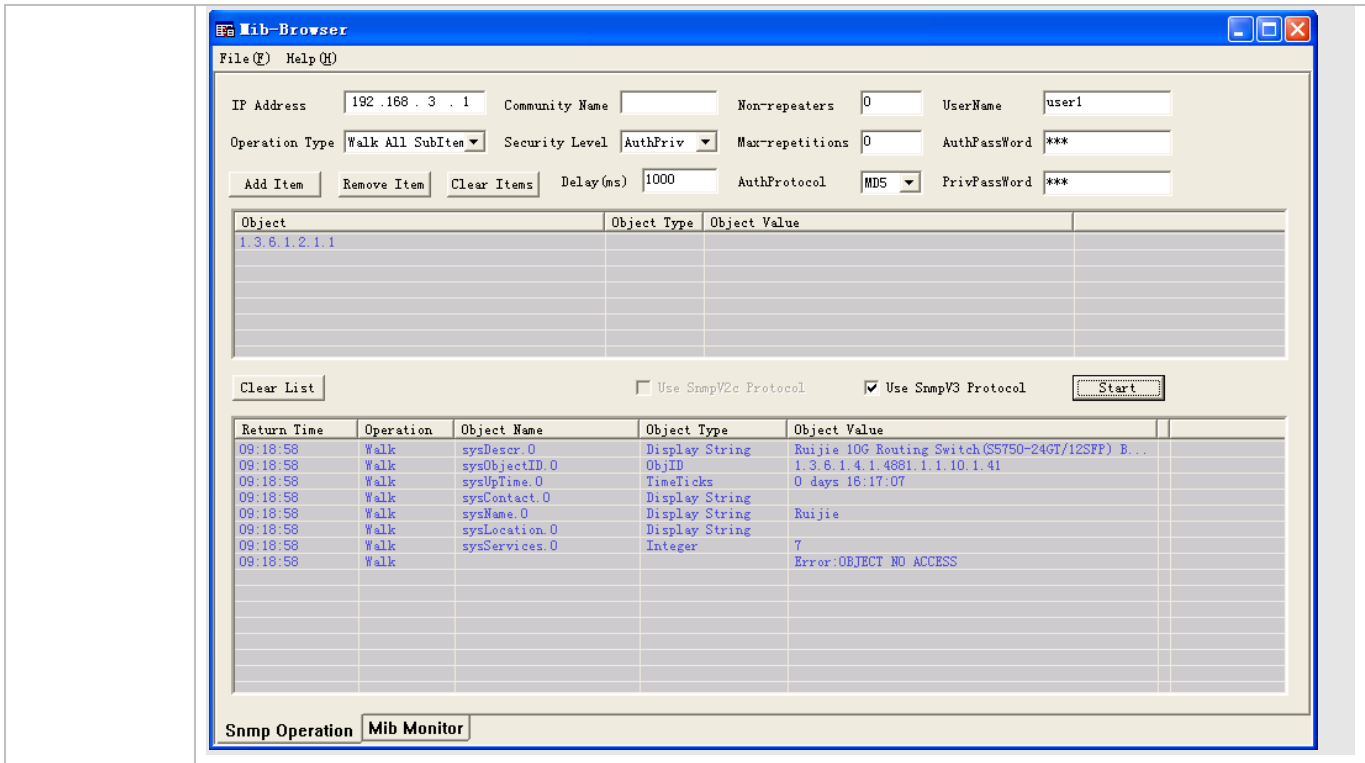
```
Ruijie# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent    active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

```
Ruijie#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 RGOS 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.

➤ **Configuring the Inform Retry Times and Request Timeout Interval**

- Optional
- The default *retry-num* is 3, and the default **timeout time** is 15 seconds.
- Configure the inform retry times and request timeout interval.


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 { <i>host-addr</i> } [traps informs] [version { 1 2c 3 { auth noauth priv }] <i>community-string</i> [udp-port <i>port-num</i>] [<i>notification-type</i>]
Parameter Description	<p><i>host-addr</i>: Address of the SNMP host.</p> <p>traps informs: Configures the host to send a trap message or an inform message.</p> <p>version: SNMP version, which can be set to V1, V2C, or V3.</p> <p>auth noauth priv: Sets the security level of V3 users.</p> <p><i>community-string</i>: Community string or user name (V3).</p> <p><i>port-num</i>: Configures the port ID of the SNMP host.</p> <p><i>notification-type</i>: Type of trap messages that are actively sent, for example, snmp.</p> <hr/> <p> If no trap type is specified, all trap messages are sent.</p>
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 [<i>notification-type</i>]
Parameter Description	<i>notification-type</i> : Enables trap notification for the corresponding events, including the following types: entity: Indicates trap notification for entity events. snmp: Enables trap notification for SNMP events. bridge: Enables trap notification for bridge events. mac-notification: Enables trap notification for MAC events.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the snmp-server host command 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 <i>interface</i>
----------------	---

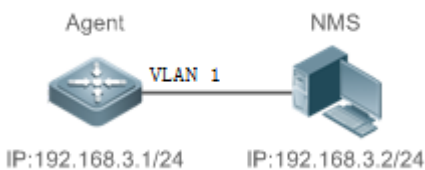
Parameter Description	<i>interface</i> : Used as the interface for the SNMP source address.
Configuration mode	Global configuration mode
Usage Guide	By default, the IP address of the interface where SNMP packets are sent is used as the source address. To facilitate management and identification, this command can be run to permanently use one local IP address as the source SNMP address.

📌 **Configuring the Inform Retry Times and Request Timeout Interval**

Command	snmp-server inform [retries <i>retry-time</i> timeout <i>time</i>]
Parameter Description	<i>retry-num</i> : Specifies the retry times for inform requests, ranging from 0 to 255. <i>Time</i> : Specifies the inform request timeout interval, ranging from 0 to 21,474,836.
Configuration mode	Global configuration mode
Usage Guide	N/A

Configuration Example

📌 **Enabling the Trap Function**

Scenario Figure 1-6	 <ul style="list-style-type: none"> The NMS manages network devices (agents) based on the community authentication mode, and network devices can actively send messages to the NMS.
Configuration Steps	<ol style="list-style-type: none"> 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. Set the IP address of the agent. Set the address of the SVI 1 interface to 192.168.3.1/24.
Agent	<pre>Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1 Ruijie(config)#snmp-server enable traps Ruijie(config)#interface vlan 1 Ruijie(config-if-VLAN 1)#ip address 192.168.3.1 255.255.255.0 Ruijie(config-if-VLAN 1)#exit</pre>

Verification	<ul style="list-style-type: none"> ● Run the show running-config command to display configuration information of the device. ● Run the show snmp command to display the SNMP status.
Agent	<pre>Ruijie# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface VLAN 1 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</pre>
	<pre>Ruijie#show snmp Chassis: 1234567890 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors</pre>

	<pre>0 General errors 0 Response PDUs 0 Trap PDUs SNMP global trap: enabled SNMP logging: disabled SNMP agent: enabled</pre>
--	--

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 Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>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.</p> <p>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.</p>

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

<p>Scenario</p> <p>Figure 1-7</p>	<p>The diagram shows a network topology with two devices connected by a line labeled 'VLAN 1'. On the left is a device labeled 'Agent' with the IP address 'IP:192.168.3.1/24'. On the right is a device labeled 'NMS' with the IP address 'IP:192.168.3.2/24'.</p>
	<p>After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.</p>

Configuration Steps	<ol style="list-style-type: none"> 1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	<pre>Ruijie(config)#enable service snmp-agent</pre>
Verification	<ol style="list-style-type: none"> 1. Run the show services command to check whether the SNMP service is enabled or disabled.
Agent	<pre>Ruijie#show service web-server : disabled web-server(https): disabled snmp-agent : enabled ssh-server : disabled telnet-server : enabled</pre>

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 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.

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 <i>text</i>
Parameter Description	<i>text</i> : String that describes the system contact mode.
Command Mode	Global configuration mode

Usage Guide	N/A
--------------------	-----

↘ Setting the System Location

Command	snmp-server location <i>text</i>
Parameter Description	<i>text</i> : String that describes system information.
Configuration mode	Global configuration mode
Usage Guide	N/A

↘ Setting the System Serial Number

Command	snmp-server chassis-id <i>text</i>
Parameter Description	<i>text</i> : Text of the system serial number, which may be 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 the Maximum Packet Length of the SNMP Agent

Command	snmp-server packet-size <i>byte-count</i>
Parameter Description	<i>byte-count</i> : Packet size, ranging from 484 bytes to 17,876 bytes.
Configuration mode	Global configuration mode.
Usage Guide	N/A

↘ Setting the UDP Port ID of the SNMP Service

Command	snmp-server udp-port <i>port-num</i>
Parameter Description	<i>port-num</i> : Specifies the UDP port ID of the SNMP service, that is, the ID of the protocol port that receives SNMP packets.
Configuration mode	Global configuration mode.
Usage Guide	Specify the protocol port ID for receiving SNMP packets.

↘ Setting the Length of a Trap Message Queue

Command	<code>snmp-server queue-length length</code>
Parameter Description	<i>length</i> : 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**

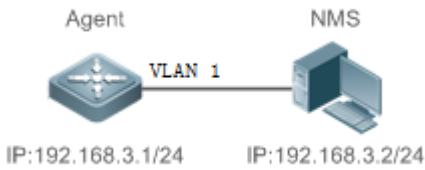
Command	<code>snmp-server trap-timeout seconds</code>
Parameter Description	<i>seconds</i> : Interval (unit: second). The value range is 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

📌 **Configuring SNMP Flow Control**

Command	<code>snmp-server flow-control pps [count]</code>
Parameter Description	<i>count</i> : 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.

Configuration Example

📌 **Setting SNMP Control Parameters**

<p>Scenario Figure 1-8</p>	 <p>The diagram illustrates a network setup where an Agent (represented by a blue square icon) and an NMS (represented by a blue server icon) are connected. The Agent has the IP address 192.168.3.1/24 and the NMS has the IP address 192.168.3.2/24. They are connected via a link labeled 'VLAN 1'.</p> <ul style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<pre>Ruijie(config)#snmp-server location fuzhou Ruijie(config)#snmp-server contact ruijie.com.cn Ruijie(config)#snmp-server chassis-id 1234567890 Ruijie(config)#interface vlan 1 Ruijie(config-if-VLAN 1)#ip address 192.168.3.1 255.255.255.0 Ruijie(config-if-VLAN 1)#exit</pre>
Verification	<ol style="list-style-type: none"> 1. Check the configuration information of the device. 2. Check the SNMP view and group information.
Agent	<pre>Ruijie# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface VLAN 1 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</pre>
	<pre>Ruijie#show snmp view v1(include) 1.3.6.1.2.1.1 default(include) 1.3.6.1 Ruijie#show snmp group groupname: user1 securityModel: v1 securityLevel:noAuthNoPriv readview: v1</pre>

```

writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
    
```

Common Errors

N/A

Common Errors

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays the SNMP status.	show snmp [mib user view group host 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, Ruijie devices can be used both as NTP clients and NTP servers. In other words, a Ruijie device can synchronize time with a time server, and be used as a time server to provide time synchronization for other devices. When a Ruijie 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.

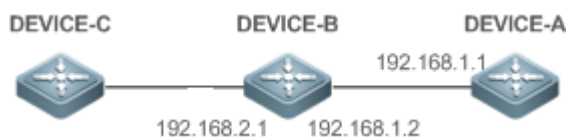
2.2.1 Synchronizing Time Based on an External Reference Clock Source

Scenario

As shown in Figure 2-1:

- 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 2-1



Deployment

Configure DEVICE-B to the NTP external reference clock mode.

2.3 Features

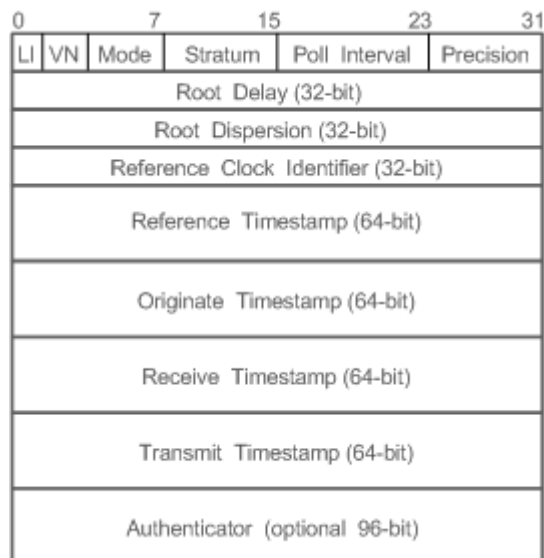
Basic Concepts

📄 NTP Packet

As defined in RFC1305, NTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure shows the format of an NTP time synchronization packet.

Figure 2-2 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 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.

2.3.1 NTP Time Synchronization

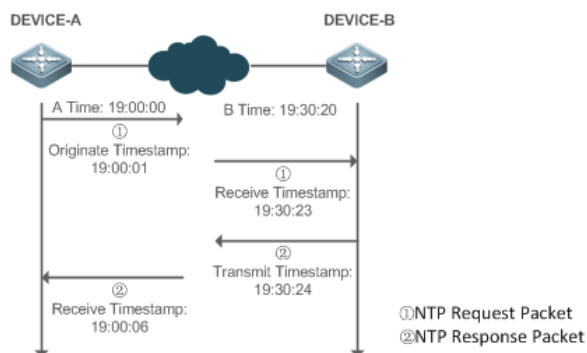
Working Principle

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 shows the format of an NTP time synchronization packet.

Figure 2-3 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 (T_0) 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 (T_1) 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 (T_2) 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 (T_3) 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 $((T_1 - T_0) + (T_2 - T_3)) / 2$.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula $(T_3 - T_0) - (T_2 - T_1)$.

📌 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.

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.

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.

2.4 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 disable NTP.
	no ntp Disables all functions of NTP and clears all NTP configurations.
Configuring NTP Security Authentication	ntp disable Disables receiving of NTP packets from a specified interface.
	 (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.

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.

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.

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.

▾ 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 { <i>ip-addr</i> <i>domain</i> ip <i>domain</i> }[version <i>version</i>][source <i>if-name</i>][key <i>keyid</i>][prefer]
Parameter Description	<p><i>ip-addr</i>: Indicates the IPv4 address of the reference clock source.</p> <p><i>domain</i>: Indicates the IPv4 domain name of the reference clock source.</p> <p><i>version</i>: Indicates the NTP version number, ranging from 1 to 3.</p> <p><i>if-name</i>: Indicates the interface type, including AggregatePort, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and Vlan.</p> <p><i>keyid</i>: Indicates the key used for communicating with the reference clock source, ranging from 1 to 4294967295.</p>

	prefer: Indicates whether the reference clock source has a high priority.
Command Mode	Global configuration mode
Usage Guide	<p>By default, no NTP server is configured. Ruijie 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.</p> <hr/> <p> If it is necessary to configure an authentication key, you must configure NTP security authentication before configuring an NTP server.</p> <hr/> <p>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.</p>

↘ Updating a Hardware Clock

Command	ntp update-calendar
Parameter Description	N/A
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

2.4.2 Configuring NTP Security Authentication

Configuration Effect

N/A

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 <i>key-id</i> md5 <i>key-string</i> [<i>enc-type</i>]
Parameter Description	<i>key-id</i> : indicates the ID of a global authentication key, ranging from 1 to 4294967295. <i>key-string</i> : indicates a key string. <i>enc-type</i> : (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 <i>key-id</i>
Parameter Description	<i>key-id</i> : Indicates the ID of a trusted key, ranging from 1 to 4294967295.
Command Mode	Global configuration mode
Usage Guide	N/A

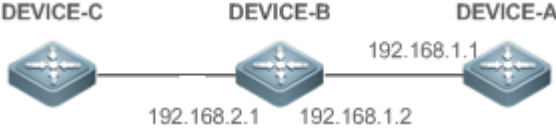
↘ **Configuring a Trusted Key for an External Reference Clock Source**

Refer to the section "[Related Commands](#)

".

Configuration Example

↘ **Security Authentication**


<p>Scenario Figure 2-4</p>	
	<ul style="list-style-type: none"> ● 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.
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
<p>DEVICE-B</p>	<pre>Ruijie#configure terminal Ruijie(config)# ntp authentication-key 1 md5 abcd Ruijie(config)# ntp trusted-key 1 Ruijie(config)# ntp server 192.168.1.1 Ruijie(config)# exit</pre>
<p>DEVICE-C</p>	<pre>Ruijie#configure terminal Ruijie(config)# ntp authentication-key 1 md5 abcd Ruijie(config)# ntp server 192.168.2.1 key 1 Ruijie(config)# exit</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● 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.

2.5 Monitoring

Displaying

Description	Command
Displays the current NTP information.	show ntp status
Displays the NTP server configuration.	show ntp server

Debugging

 System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables debugging.	debug ntp
Disables debugging.	no debug ntp

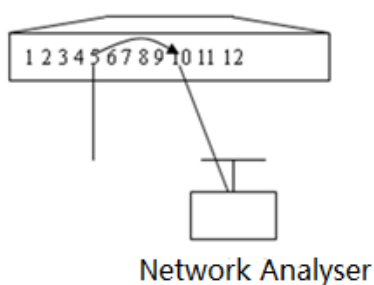
3 Configuring SPAN and RSPAN

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 3-1 SPAN Configuration Instance



The SPAN function is mainly applied in network monitoring and troubleshooting scenarios, to monitor network information and rectify network faults.

3.2 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.

3.2.1 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: Indicates that the SPAN destination port only receives packets mirrored from the SPAN source port and discards other packets if this option is disabled, and receives both packets mirrored from the SPAN source port and packets from non-source ports if this option is enabled, that is, the communication between this destination port and other devices is not affected.

When the SPAN destination port is configured, the relevant function is disabled by default if **encapsulation replicate** or **switch** is not configured.

3.3 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.

3.3.1 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.

- If the switch function is disabled on a SPAN 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.

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, or when configuring a specified VLAN or some VLANs as a data source or data sources of SPAN.

▾ 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 (or a VLAN is specified as the data source of SPAN) 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 <i>session-num</i> source interface <i>interface-id</i> [both rx tx]
Parameter Description	<p><i>session-num</i>: Indicates the ID of a SPAN session.</p> <p><i>interface-id</i>: Indicates the interface ID.</p> <p>both: Indicates that packets in the input and output directions are monitored. It is the default value.</p> <p>rx: Indicates that packets in the input direction are monitored.</p> <p>tx: Indicates that packets in the output direction are monitored.</p>
Command Mode	Global configuration mode
Usage Guide	N/A

▾ Configuring a SPAN Destination Port

Command	monitor session <i>session-num</i> destination interface <i>interface-id</i> [switch]
Parameter Description	<i>session-num</i> : Indicates the ID of a SPAN session. <i>interface-id</i> : 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 3-2	
Configuration Steps	<ul style="list-style-type: none"> As shown in Figure 3-2, 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	<pre>Ruijie# configure Ruijie(config)# vlan 1 Ruijie(config-vlan)# exit Ruijie(config)# interface vlan 1 Ruijie(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0 Ruijie(config-if-VLAN 1)# exit Ruijie(config)# monitor session 1 source interface gigabitEthernet 0/1 Ruijie(config)# monitor session 1 destination interface gigabitEthernet 0/2</pre>
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	<pre>Ruijie# show monitor sess-num: 1 span-type: LOCAL_SPAN src-intf: GigabitEthernet 0/1 frame-type Both dest-intf: GigabitEthernet 0/2</pre>

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 Monitoring

Displaying

Description	Command
Displays all mirroring sessions existing in the system.	show monitor
Displays a specified mirroring session.	show monitor session <i>session-id</i>

Debugging

 System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs SPAN.	debug span