Ruijie RG- WLAN Series Access Point

AP_RGOS 11.9(6)W3B4

Configuration Guide

Document Version: V1.1
Date: December 19, 2023
Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

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

Trademark  and  are owned by Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. Conversions

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

3. Note

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

Configuring Basic Configuration

1. Configuring CLI
2. Configuring Basic Management
3. Configuring Line
4. Configuring HTTP
5. Configuring Syslog
6. Configuring Software Upgrade
7. Configuring Time Range

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.

1.2 Applications

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

1.2.1 Configuring and Managing Network Devices Through CLI

Scenario

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

Figure 1-1

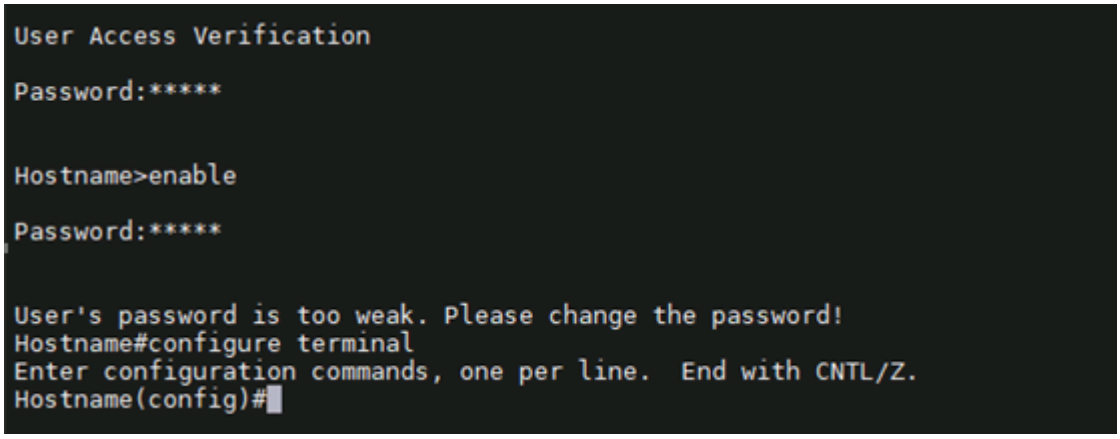


Remarks	A is the network device to be managed. PC is a terminal.

Deployment

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

Figure 1-2



1.3 Features

Overview

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

1.3.1 Accessing CLI

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

1.3.2 Command Modes

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

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

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

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

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

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

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
Global configuration (Global configuration mode)	In Privileged EXEC mode, run the **configure** command to enter global configuration mode.	Hostname(config)#	Run the **exit** or **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **interface** command to enter interface configuration mode. When using the **interface** command, you must specify the interface. Run the **vlan** *vlan_id* command to enter VLAN configuration mode.	Using commands in this mode will affect the global parameters of the network device.
Interface configuration (Interface configuration mode)	In global configuration mode, run the **interface** command to enter interface configuration mode.	Hostname(config-if-GigabitEthernet 0/1)#	Run the **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **exit** command to return to global configuration mode. When using the **interface** command, you must specify the interface.	Use this configuration mode to configure various interfaces of the network device.
Config-vlan (VLAN configuration mode)	In global configuration mode, run the **vlan** *vlan_id* command to enter VLAN configuration mode.	Hostname(config-vlan)#	Run the **end** command, or press **Ctrl+C** to return to the Privileged EXEC mode. Run the **exit** command to return to global configuration mode.	Use this configuration mode to configure VLAN parameters.

1.3.3 System Help

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

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

For example

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

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

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

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

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

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

For example

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

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

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

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

For example

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

1.3.4 Abbreviated Commands

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

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

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

1.3.5 No and Default Options of Commands

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

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

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

1.3.6 Prompts Indicating Incorrect Commands

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

The following table lists the common CLI error messages.

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

1.3.7 History Commands

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

The methods are described in the following table.

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

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

1.3.8 Featured Editing

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

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

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

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

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

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

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

The default screen width is 80 characters.

1.3.9 Searching and Filtering of the Show Command Output

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

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

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

Searched contents are case sensitive.

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

Command	Description

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

To search or filter the output of the **show** command, you must enter a vertical line (|). A maximum of 32 regular expressions can be configured to filter the command output. After the vertical line, select the searching or filtering rules and contents (character or string). Searched and filtered contents are case sensitive.

```
Hostname#show running-config | include interface
interface GigabitEthernet 0/0
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10 Command Alias

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

Configuration Steps

↘ Displaying Default Alias

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

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

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

These default aliases cannot be deleted.

Configuring a Command Alias

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

Displaying Settings of Command Aliases

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

Notes

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

Configuration Example

Defining an Alias to Replace the Entire Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the default route configuration command **ip route** *0.0.0.0 0.0.0.0 192.168.1.1.*
	Hostname#configure terminal Hostname(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
Verification	● Run the **show alias** command to check whether the alias is configured successfully. Hostname(config)#show alias Exec mode alias: h help p ping s show u undebug

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

Defining an Alias to Replace the Front Part of a Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the front part "**ip route**" of the default route configuration command.
	Hostname#configure terminal Hostname(config)#alias config ir ip route
Verification	● Run the **show alias** command to check whether the alias is configured successfully. Hostname(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route
	● Enter the alias "ir" and then the later part of the command "0.0.0.0 0.0.0.0 192.168.1.1". ● Run the **show ap-config running** command to check whether the configuration is successful.
	Hostname(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1

	Hostname(config)#show running Building configuration... ! alias config ir ip route //Configuring an alias ! ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" and the later part of the command are entered !

System Help

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

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

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

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

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

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

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

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

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

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

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

1 Configuring Basic Management

1.1 Overview

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

1.2 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.

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 stored in the batch file.

1.2.1 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.

Enabling Line Password Protection

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

1.2.2 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 After AAA Is Enabled

- After AAA is enabled, run the **login access non-aaa** command in global configuration mode to configure non-AAA authentication for line-based login.
- 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.

1.2.3 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. 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.

Configuring a Command Prompt

- Run the **prompt** command.

Configuring Daily Notification

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

Configuring a Login Banner

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

Configuring the Console Baud Rate

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

1.2.4 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, a component process is restarted, and a hot patch is running, the configurations collected during this period may be inaccurate due to the component unstable state. For example, the configurations of a component may not be missing initially but can be displayed later.

Startup Configurations

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

⚠ The startup-config file copied to the device from an external environment only supports UTF-8 (without BOM) encoding.

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 or all interfaces.

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.

1.2.5 Telnet

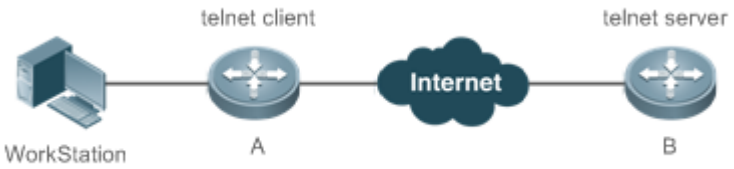
Working Principle

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 Figure 1-1, a user with a PC connects to Network Device A by using the terminal emulation or Telnet program and then logs in to Network Device B by using the **telnet** command to perform configuration management.

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

Figure 1-1



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 through Telnet.

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.

1.2.6 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.

1.2.7 Running Batch File Commands

It may take a long time to enter many commands on the CLI for system function management. This process is prone to errors and omissions. Put the commands in a batch file according to configuration steps. Executing the file will complete all configurations.

You can specify the name and content of the batch file on your PC and transfer the file to the flash memory of the device through TFTP. The content of the batch file simulates user input. Therefore, the content must be edited according to the configuration sequence of the CLI commands. For some interactive commands, the responses must be written in the batch file to ensure normal running of the commands.

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

Related Configuration

Running Batch File Commands

- Run the **execute** command to execute the commands in a batch file.
- Use this command to configure multiple commands in batch for a function, simplifying user operations.

1.3 Configuration

Configuration	Description and command	
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 command-cache	Enables the command cache.
	enable	Raises a user privilege level.
	login privilege log	Outputs the logs after the user privilege level is raised.
	disable	Lowers a user privilege level.
	privilege	Configures command privilege levels.
	password	Specifies a line password.
	login	Enables line password protection.
	(Optional) It is used to configure different login modes and authentication methods.	

Configuration	Description and command	
Configuring Login and Authentication	**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 after 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.
	ip telnet source-interface *interface-name*	Specifies the IP address of the interface as the source IP address of the Telnet session.
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 exec *c message c*	Customizes a welcome prompt indicating that a user has entered the user EXEC mode of a line.
	banner incoming *c message c*	Configures a prompt indicating the establishment of a reverse Telnet session.
	banner motd	Configures daily notification.
	banner login *c message c*	Configures a login banner.
	banner prompt-timeout *c message c*	Configures the prompt-timeout message to notify timeout.
	banner slip-ppp *c message c*	Configures the slip-ppp message for the SLIP/PPP session.
	exec-banner	Configures Display of an EXEC banner for a specific line.
	motd-banner	Configures Display of a MOTD banner for a specific line.
	speed	Configures the Console baud rate.
	write [**memory** | **terminal**]	Saves the system configurations (running-config) to a specific directory.

Configuration	Description and command	
	username import *filename*	Imports user information from a file.
	username export *filename*	Exports user information to a file.
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 batch file commands.	
	execute { [**flash:** } *filename*	Runs the batch file commands.

1.3.1 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.

Enabling the Command Cache

- Optional.
- Perform this configuration when you need to ensure that the batch commands are executed continuously without command loss.

Raising/Lowering a User Privilege Level

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

Enabling Line Password Protection

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

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

Verification

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

Related Commands

Configuring a Simple Encrypted Password

Command	**enable password** [**level** *level*] [{ *password* | { **0** [*password*] | **7** *encrypted-password* } }]
Parameter Description	*level*: Indicates a specific user level. *password:* Indicates the password used to enter privileged EXEC mode. *0:* Indicates that the password is entered in cleartext. . Indicates that the password is entered in cyphertext. *encrypted-password:* Indicates the password text, which must contain case-sensitive English letters and digits. ⓘ Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.

Command Mode	Global configuration mode
Usage Guide	Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured. If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password. If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed. If you configure a non-encrypted password, interactive password and command confirmation are supported. ⚠ If you specify an encryption type and enter a password in cleartext, you cannot re-enter privileged EXEC mode. An encrypted password cannot be retrieved once lost. You have to configure a new password.

Configuring a Secure Encrypted Password

Command	**enable secret** [**level** *level*] [{ [**0**] [*password*] | { **5** | **8** } *encrypted-secret* }]
Parameter Description	*level*: Indicates a specific user level. **0**: Specifies the cleartext password. *password*: Indicates the cleartext password used to enter the privileged EXEC mode. The password is a string of 1 to 126 characters. { **5** | **8** } *encrypted-secret*: **5** indicates that a password encrypted using the MD5 irreversible encryption algorithm is saved as an encrypted password. **8** indicates that a password encrypted using the SHA-256 irreversible encryption algorithm is saved as an encrypted password.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure passwords for different privilege levels.

Enabling the Command Cache

Command	**enable command-cache**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the command cache mode. After the command is configured, clients need to be reconnected for the configuration to take effect. ⚠ To ensure that the commands executed on the newly connected client are not overwritten by the commands being executed on the cache client, the commands should be executed on the newly connected client after being executed on the cache client. Therefore, the command execution on the newly connected client may be suspended. ⚠ After the cache mode is enabled, a maximum of 10,240 bytes of commands can be cached locally. The cache execution requires the running of the client. If the client is frequently disconnected and reconnected and a large number of commands are executed after the

	cache function is enabled, the number of clients in use may reach the upper limit. This affects the running of other clients. Therefore, this function is not recommended when a large number of commands are executed continuously and frequently for a long time. After the cache mode is enabled, the client numbering mode changes. Obtain the available client number in sequence instead of the minimum available client number from the current configured range. This may affect the display of VTY line number after the **show users** command is executed.

Raising a User Privilege Level

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

Lowering a User Privilege Level

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

Configuring Command Privilege Levels

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

Specifying a Line Password

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

Parameter Description	**0**: Indicates to configure a password in cleartext. *password*: Indicates the cleartext password for remote line-based login. The password is a string of 1 to 25 characters. **7** *encrypted-password*: Indicates the password is a string of ciphertext characters.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Line Password Protection

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

Configuration Example

Configuring Command Authorization

Scenario	Assign privilege level 1 to the **reload** command and its subcommands and configure level 1 as the valid level (by configuring the **test** password).
Configuration Steps	● Assign privilege level 1 to the **reload** command and its subcommands.
	Hostname# configure terminal Hostname(config)# privilege exec all level 1 reload Hostname(config)# enable secret level 1 0 test Hostname(config)# end
Verification	● Check whether the **reload** command and its subcommands are accessible at level 1.
	Hostname# disable 1 Hostname> reload ? at reload at<cr>

1.3.2 Configuring Login and Authentication

Configuration Effect

- Establish line-based login identity authentication.
- Run the **telnet** command on a network device to log in to a remote device.

- Close an established connection if no output is detected during the timeout time.
- Disconnect an established session connecting to a remote host and restore the host to Idle if no output is detected during the timeout time.
- Lock a terminal to deny access. When a user enters any character on the locked terminal, the password prompt is displayed. The terminal will be automatically unlocked if the entered password is correct.

Configuration Steps

Configuring Local User Information

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

Configuring Local Authentication for Line-Based Login

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

Configuring AAA Authentication for Line-Based Login

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

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

- Optional.
- After AAA is enabled, run the **login access non-aaa** command in global configuration mode to configure non-AAA authentication for line-based login.
- Perform this configuration on each 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.

Verification

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

Related Commands

Configuring Local User Information

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

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

Configuring Local Authentication for Line-Based Login

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

Configuring AAA Authentication for Line-Based Login

Command	**login authentication** { **default** | *list-name* }
Parameter Description	**default:** Indicates the default authentication method list name. *list-name*: Indicates the optional method list name.
Command Mode	Line configuration mode

Usage Guide	Use this command to configure AAA authentication for line-based login in the case that AAA is enabled. The AAA authentication methods, including RADIUS authentication, local authentication, and no authentication, are used during the authentication process.

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

Command	**login access non-aaatelnet** *host* [*port*] [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }]
Parameter Description	N/A
Command Mode	Global configuration mode
User Guide Parameter Description	To perform non-AAA authentication for a line when AAA security service is enabled, run this command. The configuration is valid for all clients. *Host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *Port*: Indicates the TCP port number of the Telnet server. The default value is 23. **/source**: Specifies the source IP address or source interface used by the Telnet client. **ip** *A.B.C.D*: Specifies the source IPv4 address used by the Telnet client. **ipv6** *X:X:X:X::X*: Specifies the source IPv6 address used by the Telnet client. **interface** *interface-name*: Specifies the source interface used by the Telnet client.

Enabling the Telnet Client Service

Command	**telnet** *host* [*port*] [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }]
Parameter Description	*host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *port*: Indicates the TCP port number of the Telnet server. The default value is 23. **/source:** Indicates the source IP address or source port used by a Telnet client. **ip** *A.B.C.D:* Indicates the source IPv4 address used by the Telnet client. **ipv6** *X:X:X:X::X:* Indicates the source IPv6 address used by the Telnet client. **interface** *interface-name*: Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

Enabling the Do Telnet Client Service

Command	**do telnet** *host* [*port*] [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }]
Parameter Description	*Host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *Port*: Indicates TCP port number of the Telnet server. The default value is 23. **/source**: Specifies the source IP address or source interface used by the Telnet client. **ip** *A.B.C.D*: Specifies the source IPv4 address used by the Telnet client. **ipv6** *X:X:X:X::X*: Specifies the source IPv6 address used by the Telnet client. **interface** *interface-name*: Specifies the source interface used by the Telnet client.
Command Mode	Privileged EXEC mode, user EXEC mode, and interface configuration mode

Usage Guide	Through the Do Telnet service, a user can log in to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

Restoring a Telnet Client Session

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

Disconnecting a Suspended Telnet Client Session

Command	**disconnect** *session-id*
Parameter Description	*session*-id: Indicates the ID of the suspended Telnet client session.
Command Mode	User EXEC mode
Usage Guide	Run this command with a Telnet client session ID to disconnect the specified Telnet client session.

Enabling the Telnet Server Service

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

Configuring the Connection Timeout Time

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

Configuring the Session Timeout Time

Command	**session-timeout** *minutes* [**output**]

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

Enabling Line-Based Terminal Lock

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

Locking a Terminal Connected to the Current Line

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

Specifies the IP address of the interface as the source IP address of the Telnet session.

Command	**ip telnet source-interface** *interface-name*
Parameter Description	*Interface-name*:: Specifies the IP address configured on the interface as the source address for the Telnet session. The interface types include aggregate interface, Gigabit interface, Loopback interface, null interface, Tunnel interface, and VLAN interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Establishing a Telnet Session to a Remote Network Device

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

	Trying 192.168.65.119 ... Open User Access Verification Password:
	Hostname# telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:
Verification	● Check whether the Telnet sessions are established to the remote network devices.

Configuring the Connection Timeout Time

Configuration Steps	● Set the connection timeout time to 20 minutes.
	Hostname# configure terminal//Enter global configuration mode. Hostname# line vty 0 //Enter line configuration mode. Hostname(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.
Verification	● Check whether the connection between a terminal and the local device is closed when no input is detected during the timeout time.

Configuring the Session Timeout Time

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

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

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

1.3.3 Configuring Basic System Parameters

Configuration Effect

- Configure basic system parameters.

Configuration Steps

Configuring the System Date and Clock

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

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

Updating the Hardware Clock

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

Configuring a System Name

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

Configuring a Command Prompt

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

Configuring Daily Notification

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

Configuring a Login Banner

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

Configuring the Console Baud Rate

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

Verification

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

Related Commands

Configuring the System Date and Clock

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

Updating the Hardware Clock

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

Configuring a System Name

Command	**hostname** *name*
Parameter Description	*name*: Indicates the system name, which must consist of printable characters and must not exceed 63 bytes.
Command Mode	Global configuration mode
Usage Guide	To restore the system name to the default, run the **no hostname** command in global configuration mode.

Configuring a Command Prompt

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

Customizing a Welcome Prompt Before Users Enter the User EXEC Mode of a Line

Command	**banner exec** *c message c*
Parameter Description	*c*: Indicates a delimiter. Spaces are not allowed in the welcome prompt. *Message:* Configures the welcome prompt.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Prompt Indicating the Establishment of a Reverse Telnet Session

Command	**banner incoming** *c message c*
Parameter Description	*c*: Indicates a delimiter. Spaces are not allowed in the prompt. *message*: Configures a prompt for the establishment of a reverse Telnet session.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Daily Notification

Command	**banner motd** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with the combination of a delimiter and a 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 cannot exceed 255 bytes.

Configuring a Login Banner

Command	**banner login** *c message c*
Parameter Description	Indicates a delimiter, which can be any character, such as “&”.
Command Mode	Global configuration mode
Usage Guide	A message must start and end with the combination of a delimiter and a 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 cannot exceed 255 bytes. Run the **no banner login** command in global configuration mode to delete the banner.

Configuring the Prompt-Timeout Message to Notify Timeout

Command	**banner prompt-timeout** *c message c*
Parameter Description	*c*: Separator of the message. Delimiters are not allowed in the message. *Message*: Contents of the message.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the slip-ppp Message for the SLIP/PPP Session

Command	**banner slip-ppp** *c message c*
Parameter Description	*c*: Separator of the message. Delimiters are not allowed in the message. *Message*: Contents of the message.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Display of EXEC Banner for a Specific Line

Command	**exec-banner**
Parameter Description	N/A
Command Mode	Line configuration mode

Usage Guide	If the **banner exec** and **banner motd** commands are configured on the device, EXEC and MOTD banners are displayed for all lines by default. To disable EXEC and MOTD banners displayed for a specific line, run the **no** form of these two commands.

Configuring Display of MOTD Banner for a Specific Line

Command	**motd-banner**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	If the **banner exec** and **banner motd** commands are configured on the device, EXEC and MOTD banners are displayed for all lines by default. To disable EXEC and MOTD banners displayed for a specific line, run the **no** form of these two commands.

Configuring the Console Baud Rate

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

Saving System Configurations (running-config) to a Specific Directory

Command	**write** [**memory** | **terminal**]
Parameter Description	**memory**: Writes system configurations to the NVRAM. It has the same effect as running the **copy running-config startup-config** command. **terminal**: Displays system configurations. It has the same effect as running the **show running-config** command.
Command Mode	Privileged EXEC mode
Usage Guide	There are alternatives to this command. But because of its widespread use and acceptance, this command has been retained. In the presence of such a device, the system automatically creates a file and writes the system configurations to the file. In the absence of such a device, for example, as the startup configuration file is specified to be in a portable storage device such as a USB flash drive or SD card, but the device is not mounted during the execution of the **write** [memory] command, the system asks you whether to save the current configurations to the default startup configuration file **config.text** and performs corresponding operations.

Importing User Information from a File

Command	**username import** *filename*

Parameter Description	*filename*: Indicates the name of the file.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Exporting User Information to a File

Command	**username export** *filename*
Parameter Description	*filename*: Indicates the name of the file.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Configuring the System Time

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

Configuring Daily Notification

Configuration Steps	● Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	Hostname(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#'. Notice: system will shutdown on July 6th.# //Ending delimiter Hostname(config)#
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:

Configuring a Login Banner

Configuration Steps	● Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.
	Hostname(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#'. Access for authorized users only. Please enter your password. # //Ending delimiter Hostname(config)#
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether the login banner is displayed before the CLI appears.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:

Configuring the Serial Port Baud Rate

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

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

Verification	● Run the **show** command to display the configuration.
	Hostname# show line console 0 //Displays the console configuration. CON Type speed Overruns * 0 CON 57600 0 Line 0, Location: "", Type: "vt100" Length: 25 lines, Width: 80 columns Special Chars: Escape Disconnect Activation ^^x none ^M Timeouts: Idle EXEC Idle Session never never

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

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

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

1.3.4 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 SSH Server, Telnet Server, and SNMP Agent Services

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

Command Mode	Global configuration mode
Usage Guide	Use this command to enable and disable specific services.

Configuration Example

Enabling the SSH Server Service

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

1.3.5 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	**reload** [**at** { *hh* [:*mm* [:*ss*]] } [*month* [*day* [*year*]]]]

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

1.3.6 Running Batch File Commands

Configuration Effect

Runs the commands in a batch file.

Configuration Steps

Running the execute Command

In the **execute** command, specify the path of the batch files to be executed.

You can specify the name and content of the batch file on your PC and transfer the file to the flash memory of the device through TFTP. The content of the batch file simulates user input. Therefore, you must edit the content according to the configuration sequence of the CLI commands. For some interactive commands, the responses must be written in the batch file to ensure normal running of the commands.

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

Related Commands

Restarting a Device

Command	**execute** { [**flash:**] *filename* }
Parameter Description	*filename*: Indicates the path of the batch file.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to execute multiple commands in batch for a function, simplifying user operations.

1.4 Monitoring

Displaying

Description	Command
Displays the current system time.	**show clock**
Displays line configurations.	**show line** { **console** *line-num* | **vty** *line-num* | *line-num* }

Displays the current running configurations of the device or the configurations on an interface.	**show running-config** [**interface** *interface*]
Displays the system information.	**show version** [**devices | module | slots**]
Displays the information about the established Telnet client instances.	**show sessions**
Displays the information of the supported diagnostic commands and the device.	**execute diagnose-cmd** { **help** | *shell-command* }
Displays system restart settings.	**show reload**
Displays the device configurations stored in the NVRAM.	**show startup-config**
Displays the host name of the device.	**show hostname**
Displays the line configurations.	**show language character-set**
Displays the service status in the current system.	**show service**

1 Configuring Line

1.1 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, TTY, AUX, and VTY.

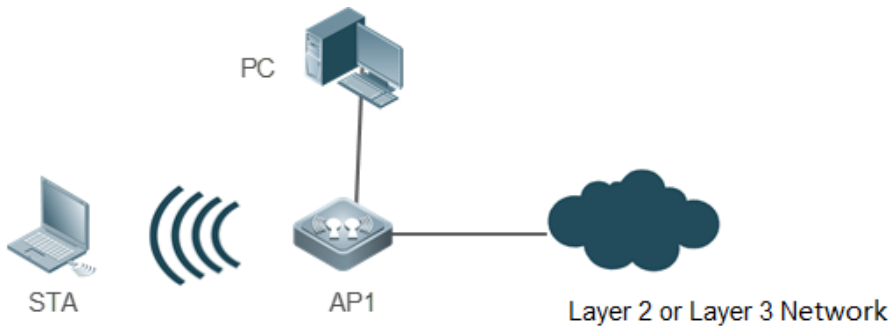
1.2 Applications

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.

1.2.1 Accessing a Device Through Console

Scenario

Figure 1-1



Remarks	AP1 is a network device to be managed. PC is a network management station.

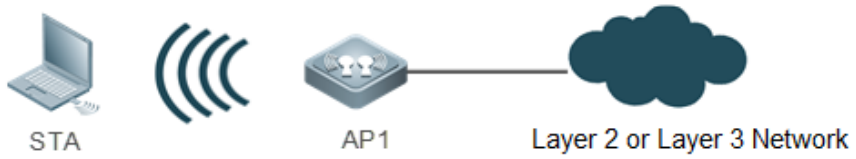
Deployment

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.

1.2.2 Accessing a Device Through VTY

Scenario

Figure 1-2



Remarks	AP1 is a network device to be managed. STA 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.

1.3 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.

1.3.1 Basic Features

Related Configuration

Configuring Terminal Lines

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

Various terminal attributes can be configured.

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.

1.4 Configuration

Configuration	Description and Command	
Entering Line Configuration Mode	⚠ (Mandatory) It is used to enter the line configuration mode.	
	line [**console** | **tty** | **vty**] *first-line* [*last-line*]	Enters the specified line configuration mode.
	line vty *line-number*	Increases or reduces the number of available VTY lines.
Configuring Line Attributes	**access-class** { *access-list-number* | *access-list-name* } { **in** | **out** }	Configures login to the terminal through IPv4 ACL
	accounting commands *level* { **default** | *list-name* }	Enables command accounting for a line.
	accounting exec { **default** | *list-name* }	Enables user access accounting for a line.
	authorization commands *level* { **default** | *list-name* }	Enables command authorization for a line.
	accounting exec { **default** | *list-name* }	Enables EXEC authorization for a line.
	disconnect-character *ascii-value*	Configures the hot key for terminal service disconnection.
	escape-character *escape-value*	Configures the character for exiting a line.
	exec	Configures the access to the CLI through a line.
	history [**size** *size*]	Enables command history for the line or configures the number of commands in the command history.
	ipv6 access-class *access-list-name* { **in** | **out** }	Configures login to the terminal through IPv6 ACL
	length *screen-length*	Configures the maximum number of lines that are displayed on a single screen for a specific line terminal.
	location *location*	Configures the location description for a specified line.
	monitor	Enables logging on terminals.

	privilege level	Configures a privilege level for line-based login.
	refuse-message [*c message c*]	Configures the prompt for refusing line-based login.
	speed *baudrate*	Configures the baud rate for a specified terminal.
	terminal escape-character *escape-value*	Configures the character for exiting the current terminal.
	terminal history [**size** *size*]	Enables command history or configures the number of commands in the command history for the line connected to the current terminal.
	terminal length *screen-length*	Configures the maximum number of lines that are displayed on a single screen on the current terminal.
	terminal location *location*	Configures the location description for the current terminal.
	terminal speed *baudrate*	Configures the baud rate for the current terminal.
	terminal width *screen-width*	Configures the maximum number of columns that are displayed in a single line on the current terminal, that is, the line width.
	timeout login response *seconds*	Configures the authentication timeout for line-based login.
	transport input { **all** | **ssh** | **telnet** | **none** }	Specifies the communication protocols supported in a line.
	vacant-message [*c message c*]	Configures the prompt for line-based logout.
	width *screen-width*	Configures the maximum number of columns that are displayed in a single line on a specified terminal, that is, the line width.

1.4.1 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.

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

Increasing/Reducing the Number of VTY Lines

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

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

Displaying Line Configuration

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

Verification

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

Configuration Example

Scenario Figure 1-3	
Configuration Steps	- Connect the PC to network device A through the Console line and enter the CLI on the PC. - Run the **show user** command to display the connection status of the terminal line.

	● Run the **show line console** 0 command to display the status of the Console line. ● Enter global configuration mode and run the **line vty** command to increase the number of VTY terminals to 36.
A	Hostname#show user Line User Host(s) Idle Location ---------- ---------- ---------- ---------- ---------- * 0 con 0 --- idle 00:00:00 --- Hostname#show line console 0 CON Type speed Overruns * 0 CON 9600 0 Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x ^D ^M Timeouts: Idle EXEC Idle Session 00:10:00 never History is enabled, history size is 10. Total input: 490 bytes Total output: 59366 bytes Data overflow: 0 bytes stop rx interrupt: 0 times Hostname#show line vty ? <0-5> Line number Hostname#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#line vty 35 Hostname(config-line)# *Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console
Verification	● After running the **show line** command, you can find that the number of terminals increases. ● Run the **show running-config** command to display the configuration.

A	Hostname#show line vty ? <0-35> Line number Hostname#show running-config Building configuration... Current configuration : 761 bytes version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78) ip tcp not-send-rst vlan 1 ! interface GigabitEthernet 0/0 ! interface GigabitEthernet 0/1 ip address 192.168.23.164 255.255.255.0 ! interface GigabitEthernet 0/2 ! interface GigabitEthernet 0/3 ! interface GigabitEthernet 0/4 ! interface GigabitEthernet 0/5 ! interface GigabitEthernet 0/6 ! interface GigabitEthernet 0/7 ! interface Mgmt 0 ! line con 0 line vty 0 35 login

	! end

1.4.2 Configuring Line Attributes

Configuration Effect

Configure line attributes in line configuration mode.

Configuration Steps

Configuring Login into the Terminal Through IPv4 ACL

Command	**access-class** { *access-list-number* | *access-list-name* } { **in** | **out** }
Parameter Description	*access-list-number*: Specifies the ACL number. Standard IP ACL number is from 1 to 99 and from 1300 to 1999. Extended IP ACL number is from 100 to 199 and from 2000 to 2699. *access-list-name*: Specifies the ACL name. **in**: Filters the incoming connections. **out**: Filters the outgoing connections.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling User Access Accounting for a Line

Command	**accounting exec** { **default** | *list-name* }
Parameter Description	*level*: Indicates the level of commands that need authorization, in the range from 0 to 15. Only authorized commands can be executed. **default**: Specifies the name of the default authentication method list. *list*-name: Indicates the name of the optional method list.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Command Authorization for a Line

Command	**authorization commands** *level* { **default** | *list-name* }
Parameter Description	**default**: Specifies the name of the default authentication method list. *list*-name: Indicates the name of the optional method list.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling EXEC Authorization for a Line

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

Parameter Description	**default**: Specifies the name of the default authentication method list. *list*-name: Indicates the name of the optional method list.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Hot Key for Terminal Service Disconnection

Command	**disconnect-character** *ascii-value*
Parameter Description	*ascii*-value: ASCII decimal value of the hot key that disconnects terminal service connections, in the range from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	This command is used to configure the hot key for disconnecting terminal connections based on requirements. The hot key for disconnecting terminal connections cannot be common ASCII values (such as a–z, A–Z, and 0–9). Otherwise, the terminal service may be abnormal.

Configuring the Character for Exiting a Line

Command	**escape-character** *escape-value*
Parameter Description	*escape-value*: ASCII value in decimal notation of the user-defined character for exiting the current terminal. The range is from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Access to the CLI Through a Line

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

Enabling Command History for the Line or Configuring the Number of Commands in the Command History

Command	**history** [**size** *size*]
Parameter Description	***size*** *size*: Configures number of commands, in the range from 0 to 256.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring Login into the Terminal Through IPv6 ACL

Command	**ipv6 access-class** *access-list-name* { **in** | **out** }

Parameter Description	*access-list-name*: Specifies the ACL name. **in**: Filters the incoming connections. **out**: Filters the outgoing connections.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Lines on a Single Screen for a Specified Line Terminal

Command	**length** *screen-length*
Parameter Description	*screen-ength*: Indicates the line height in the range from 0 to 512.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Location Description for a Specified Line

Command	**location** *location*
Parameter Description	*location*: Indicates the location description of the current line.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Logging on Terminals

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

Configuring a Privilege Level for Line-based Login

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

Configuring the Prompt for Refusing Line-based Login

Command	**refuse-message** [*c message c*]
Parameter Description	N/A

Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Baud Rate for a Specified Line Terminal

Command	**speed** *baudrate*
Parameter Description	*baudrate*: Indicates the baud rate in the range from 9600 to 115200.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Character for Exiting the Current Terminal

Command	**terminal escape-character** *escape-value*
Parameter Description	*escape*-value: ASCII value in decimal notation of the user-defined character for exiting the current terminal. The range is from 0 to 255.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Enabling Command History for the Line Connected to the Current Terminal or Configuring the Number of Commands in the Command History

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

Configuring the Maximum Number of Lines Displayed on a Single Screen on the Current Terminal

Command	**terminal length** *screen-length*
Parameter Description	*screen-ength*: Indicates the line height in the range from 0 to 512.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring Location Description for the Current Terminal

Command	**terminal location** *location*
Parameter Description	*location*: Indicates the location description of the current line.
Command Mode	Privileged EXEC mode

Usage Guide	N/A

Configuring the Baud Rate for the Current Terminal

Command	**terminal speed** *baudrate*
Parameter Description	*baudrate*: Indicates the baud rate in the range from 9600 to 115200.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Line Width on the Current Terminal

Command	**terminal width** *screen-width*
Parameter Description	*screen*-width: Indicates the maximum number of columns displayed in a single line, that is, the line width. The range is from 0 to 256.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Authentication Timeout for Line-based Login

Command	**timeout login response** *seconds*
Parameter Description	**response**: Indicates the time period during which a line waits for a user to enter any message. *seconds*: Indicates the authentication timeout duration for line-based login. The value is in seconds ranging from 1 to 300.
Command Mode	Line configuration mode
Usage Guide	N/A

Specifying the Communication Protocols Supported in a Line

Command	**transport input** { **all** | **ssh** | **telnet** | **none** }
Parameter Description	***all***: Indicates that all protocols are supported by default. ***ssh***: Indicates that SSH protocol is supported. ***telenet***: Indicates that Telnet protocol is supported. ***none***: Indicates that no protocol is supported for communication in a line.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring the Prompt for Line-based Logout

Command	**vacant-message** [*c message c*]
Parameter Description	*c*: Indicates the delimiter of the prompt for line-based logout, which is not allowed within the message message: Indicates a prompt for line-based logout.
Command Mode	Line configuration mode

Usage Guide	N/A

Configuring the Line Width on a Specified terminal

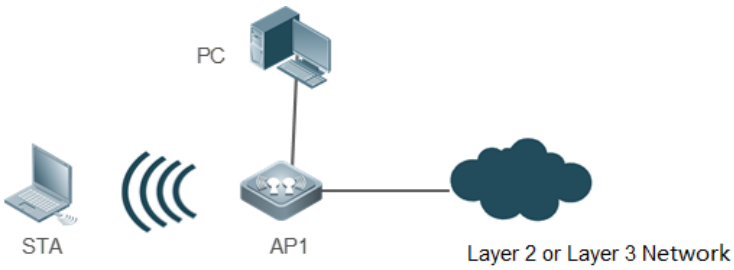
Command	**width** *screen-width*
Parameter Description	*screen*-width: Indicates the maximum number of columns displayed in a single line, that is, the line width. The range is from 0 to 256.
Command Mode	Line configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the Baud Rate for a Line

Scenario Figure 1-4	
Configuration Steps	● Connect the PC to the console port of device A with an Ethernet cable and enter the CLI. ● Enter global configuration mode and configure the baud rate for a line. ● Run the **show line console 0** command to check the console line status.
A	Hostname#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#line console 0 Hostname(config-line)#speed 115200 Hostname#show line console 0 CON Type speed Overruns * 0 CON 115200 0 Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x none Timeouts: Idle EXEC Idle Session 00:10:00 never History is enabled, history size is 10. Total input: 636 bytes

	Total output: 30498 bytes Data overflow: 0 bytes stop rx interrupt: 0 times
Verification	● Run the **show running-config** command to check the configuration.
A	Hostname#show line vty ? <0-35> Line number Hostname#show running-config Building configuration... Current configuration : 761 bytes version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78) ip tcp not-send-rst vlan 1 ! interface GigabitEthernet 0/0 ! interface GigabitEthernet 0/1 ip address 192.168.23.164 255.255.255.0 ! interface GigabitEthernet 0/2 ! interface GigabitEthernet 0/3 ! interface GigabitEthernet 0/4 ! interface GigabitEthernet 0/5 ! interface GigabitEthernet 0/6 ! interface GigabitEthernet 0/7 ! interface Mgmt 0 ! end

1.5 Monitoring

Clearing

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

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

Displaying

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

1 Configuring the HTTP Service

1.1 Overview

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

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

Protocols and Standards

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

1.2 Features

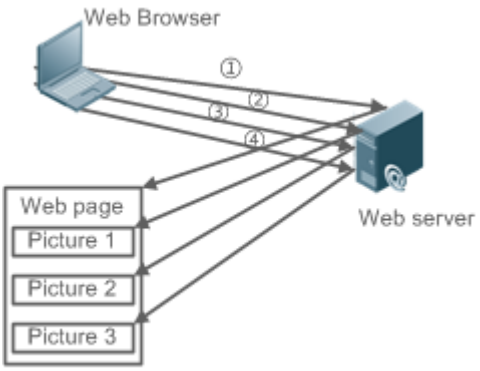
Basic Concepts

↘ HTTP Service

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

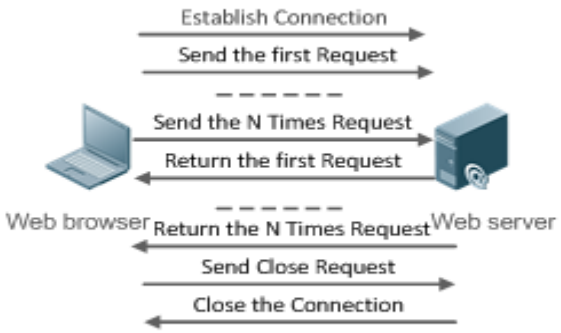
For example, a web page my need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is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

Figure 1-1



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 1-2



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

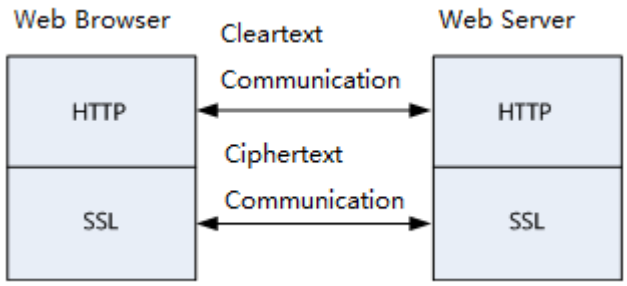
Which HTTP version will be used by a device is decided by the Web browser.

HTTPS Service

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

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

Figure 1-3



Features

Feature	Description
HTTP Service	Users log in to devices through Web pages to configure and manage devices.
HTTP Redirection to HTTPS	When a user accesses the Web page through HTTP, HTTP is automatically redirected to HTTPS.
HTTPS Service Certificate	A new self-signed HTTPS service certificate is generated or a third-party certificate is installed.

1.2.1 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.

1.2.2 HTTP Redirection to HTTPS

The device redirects the browser access request to HTTPS when a user accesses the Web management service through the HTTP.

Working Principle

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

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

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

1.2.3 HTTPS Service Certificate

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

Working Principle

- The device generates a self-signed certificate as the HTTPS service certificate upon its first startup. Users can enable the device to generate a new self-signed certificate again or install a trust certificate issued by the certificate authority.
- The server delivers the certificate to the browser after the browser connects to the server through HTTPS.
- The browser checks the certificate delivered by the server to see whether the certificate user matches the address accessed, whether the certificate is in the validity period, and whether the certificate issuer is trusted by the browser. If not, the browser displays a security prompt, asking for user's confirmation before the user accesses the server.

1.3 Configuration

Configuration	Description and Command	
Configuring the HTTP Service	⚠ (Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	webmaster level	Configures HTTP authentication information.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring HTTP Redirection to HTTPS	⚠ (Optional) It is used to enable automatic HTTP redirection to HTTPS.	
	web-server http redirect-to-https	Configures HTTP redirection to HTTPS.
Configuring an HTTPS Service Certificate	⚠ (Optional) It is used to replace a HTTPS service certificate.	
	web-server https generate self-signed-certificate	Generates a new self-signed HTTPS service certificate again.
	web-server https certificate	Installs an HTTPS service certificate.

1.3.1 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

- The HTTP service is disabled by default.
- Run the **enable service web-server** command to enable HTTP service functions including HTTP service and HTTPS service.
- Users log in to devices through Web pages to configure and manage the devices only after HTTP service is enabled.

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

Configuring HTTP Authentication Information

- If there is no special requirement, you can log in to the Web page by using the default username and directly update authentication information through the Web browser.
- By default, the level, username and password are set to **0**, **admin**, and **admin** respectively.
- Run the **webmaster level** command to configure a username and a password for authentication.
- If this command, is configured, you need to enter the configured username and password for authentication before logging in to the Web page.

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }
Parameter Description	*privilege-level*: Permission level bound to a user. *name*: User name. *password*: User password. **0 | 7**: Password encryption type. 0: no encryption; 7: simple encryption. The default value is **0**. *encrypted-password*: Password text.

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

Configuring an HTTP Service Port

- To change an HTTP service port, configure the HTTP service port.
- If there is no special requirement, the default HTTP service port 80 can be used for access.
- Run the **http port** command to configure an HTTP service port number. The value range is 80 and from 1025 to 65535.
- Configure an HTTP service port number to reduce attacks initiated by unauthorized users on HTTP service.

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

Configuring an HTTPS Service Port

- 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.
- Run the **http secure-port** command to configure an HTTPS service port number. The value range is 443 and from 1025 to 65535.
- Configure an HTTPS service port number to reduce attacks initiated by unauthorized users on HTTPS service.

Command	**http secure-port** *port-number*
Parameter Description	*port-number*: 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.

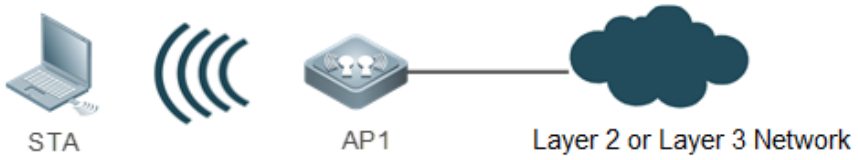
Verification

- 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.

Configuration Example

Managing one 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 and HTTPS 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 1-4	
Configuration Steps	• Enable the HTTP and HTTPS services at the same time. • Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.
AP	A#configure terminal A(config)# enable service web-server A(config)# http port 8080 A(config)# http secure-port 4430
Verification	Check HTTP configurations.
AP	A# show web-server status http server status: enabled http server port: 8080 https server status:enabled https server port: 4430

Common Errors

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

1.3.2 Configuring HTTP Redirection to HTTPS

Configuration Effect

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

Configuration Steps

↘ Configuring HTTP Redirection to HTTPS

- Automatic HTTP redirection to HTTPS is disabled by default.
- Run the **web-server http redirect-to-https** command to enable automatic HTTP redirection to HTTPS.
- After automatic HTTP redirection to HTTPS is enabled, HTTP service requests can be redirected to HTTPS service to improve security and reduce information leak risk.

Command	**web-server http redirect-to-https**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When a user uses a browser to access the Web management system through HTTP after automatic HTTP redirection to HTTPS is configured, the Web server address automatically redirects to HTTPS. Run the **no web-server http redirect-to-https** or **default web-server http redirect-to-https** command to disable automatic HTTP redirection to HTTPS. ℹ HTTP service is automatically redirected to HTTPS service only when the HTTP and HTTPS services are enabled. ℹ Whether this command is supported is subject to actual products. ⚠ If an IP address to be accessed is a Network Address and Port Translation (NAPT) address, the redirection function may fail. To access the device through HTTP, disable the NAPT feature; to access the device through HTTPS, use HTTPS directly.

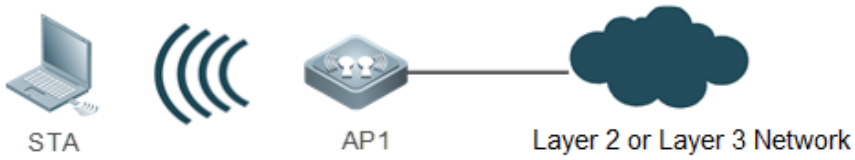
Verification

- Enter **http://IP address of the device: service port** in the address bar of a browser to check whether the browser is redirected to **https://IP address of the device: service port**.
- Run the **show web-server status** command to check whether automatic HTTP redirection to HTTPS is enabled.

Configuration Example

↘ Logging In to the Web Management System of a Device Through a Browser

- To improve security, HTTP is automatically redirected to HTTPS when a user accesses the page through HTTP,

Scenario **Figure 1-6**	
Configuration Steps	• Enable both the HTTP and HTTPS services. • Configure HTTP redirection to HTTPS.
AP	A#configure terminal A(config)# enable service web-server A(config)# web-server http redirect-to-https
Verification	• Check the Web service status. • Enter **http://IP address of the device** in the address bar of a browser to check whether the browser is redirected to **https://IP address of the device**.
AP	A(config)#show web-server status http server status: enabled http server port: 80 https server status:enabled https server port: 443 http redirect to https: true

1.3.3 Configuring an HTTPS Service Certificate

Configuration Effect

The devices use an automatically generated self-signed certificate as the HTTPS service certificate by default. After an HTTPS service certificate is configured, the device generates a self-signed certificate again or uses the certificate assigned by the certificate authority.

Configuration Steps

↘ Regenerating a Self-Signed HTTPS Service Certificate

- The HTTPS service uses the self-signed certificate by default.
- Run the **web-server https generate self-signed-certificate** command to generate a self-signed HTTPS service certificate.

Command	**web-server https generate self-signed-certificate**
Parameter Description	N/A

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

Installing the HTTPS Certificate

- The HTTPS service uses the self-signed certificate by default.
- Run the **web-server https certificate** command to install the HTTPS service certificate issued by the certificate authority.
- An HTTPS certificate issued by a trusted certificate authority can be installed on the device to eliminate the warning that the browser's certificate is untrusted when you access the device through HTTPS.

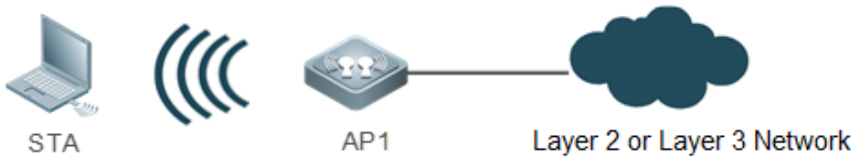
Command	**web-server https certificate { pem** *cert-filename* **private-key** *key-filename* **} | { pfx** *cert-filename* **} [password** *password-text* **]**
Parameter Description	**pem**: Imports the certificate file and private key file in the pem. format. **pfx**: Imports the certificate file in the pfx. format from which a private key is exported. *cert-filename*: Indicates the file name in the **flash:** partition. *key-filename*: in the **flash:** partition. Indicates the private key file name **password** *password-text*: Indicates the decryption password of the private key file or decryption password of the private key exported from the pfx certificate.
Command Mode	Global configuration mode
Usage Guide	Run the **copy** command to copy the certificate/private key file to the **flash:** partition before running the command to install the third-party HTTPS service certificate. After installation, you can delete the certificate/private key file from the **flash:** partition. Run the **no web-server https certificate** command to remove the installed HTTPS service certificate. After deletion, the HTTPS service will use the self-signed certificate. This command is not displayed in the configuration (running-config). The supported configuration may vary depending on actual products. After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

Verification

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

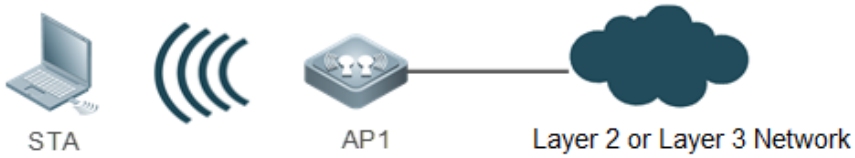
Configuration Example

Regenerating a Self-Signed Certificate

Scenario **Figure 1-6**	
Configuration Steps	● Configure the device to generate a self-signed certificate again.
AP	A#configure terminal A(config)# web-server https generate self-signed-certificate RSA key modulus bits (1024~4096) [2048]: Common Name (e.g. server IP) [Self-Signed-600B16C2]: % Generate self-signed certificate successfully
Verification	● Run the **show web-server https certificate information** command to display the information of the certificate.
AP	A#show web-server https certificate information Source: Default Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: sha256WithRSAEncryption Issuer: CN=Self-Signed-600B16C2 Validity Not Before: Feb 28 05:49:39 2019 GMT Not After : Feb 25 05:49:39 2029 GMT Subject: CN=Self-Signed-600B16C2 Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: .....(omitted)

Installing the Third-Party HTTPS Service Certificate

- The name of the certificate file is **usercert.pfx**, and the password of the private key file is **123456.** TFTP server is enabled on the PC and the certificate file is in the directory of TFTP server.

Scenario **Figure 1-6**	
Configuration Steps	● Run the **copy** command to copy the certificate/private key file to the **flash:** partition. ● Run the **web-server https certificate** command to install the HTTPS service certificate.
AP	A# copy tftp://192.168.1.1/usercert.pfx flash:usercert.pfx Press Ctrl+C to quit ! Copy success. A#configure terminal A(config)# web-server https certificate pfx usercert.pfx password 123456 *Feb 28 14:38:37: %HTTPD-4-CERT_CHANGE: HTTPS certificate changed. % The certificate was successfully installed.
Verification	● Run the **show web-server https certificate information** command to display the information of the certificate.
AP	A#show web-server https certificate information Source: Installed Certificate: Data: Version: 3 (0x2) Serial Number: 4 (0x4) Signature Algorithm: sha1WithRSAEncryption Issuer: C=CN, CN=mytestCA Validity Not Before: Jan 23 08:36:21 2019 GMT Not After : Jan 23 08:36:21 2020 GMT Subject: C=CN, CN=test-cert-2 Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: .....(omitted)

1.4 Monitoring

Displaying

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

1 Configuring Syslog

1.1 Overview

Status changes (such as link up and down) or abnormal events may occur anytime. The devices 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

1.2 Applications

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

1.2.1 Sending Syslogs to the Console

Scenario

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

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

Figure 1-1 shows the network topology.

Figure 1-1 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.

1.2.2 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 syslogs from the source interface Loopback 0 to the log server.
3. Set the logs that cannot be received. Send the logs of IP assignment by DHCP to the log server.
4. Set the warning (Level 4) logs that can be sent to the log server.

Figure 1-2 Networking Topology of Sending Syslogs to the Log Server



Deployment

Configure the device as follows:

1. Set the IPv4 address of the server to 10.1.1.1.
2. Set the source interface of logs sent to the log server to Loopback 0.
3. Set the sending mode of logs sent to the log server to audit mode.
4. Configure the log filtering rules in audit mode to allow for the sending of the logs of IP assignment by DHCP and the forth-level (warning) logs to the log server.

1.3 Features

Basic Concepts

Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

Levels of Syslogs

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

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

The following table describes the log levels.

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

Output Direction of Syslogs

Output directions of syslogs include Console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions.

The following table describes output directions of syslogs.

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

RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

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

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

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

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

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

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

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

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

The following describes each field in the log in details:

1. 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)

2. 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.

3. Timestamp

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

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

The two timestamp formats are described as follows:

- Datetime format

The datetime format is as follows:

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

The following table describes each parameter of the datetime.

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

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

- Uptime format

The uptime format is as follows:

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

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

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. By default, this field is not displayed. You can run a command to display or hide this field.

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 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.

8. 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 Hostname 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. 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). Device' 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.

1.3.1 Logging

Enable or disable the logging, redirection 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.

1.3.2 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 the old format (RFC3164 log format) is enabled, the logging delay-send, logging policy, and logging statistic commands that are applicable only to the RFC5424 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.

1.3.3 Logging Direction

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

Related Configuration

Configuring Synchronization of User Input and Log Output

The synchronization of user input and log output is disabled by default.

Run the **logging synchronous** command to enable the synchronization of user input and log output in line configuration mode to prevent interruption of user input.

Configuring the Log Rate Limit

By default, no log rate limit is configured.

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

Configuring the Level of Logs Sent to the Console

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

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

Sending Logs to the Monitor Terminal

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

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

Configuring the Level of Logs Sent to the Monitor Terminal

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

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

Writing Logs into the Memory Buffer

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

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

Sending Logs to the Log Server

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

Run the **logging server** { *ip-address* | **IPv6** *IPv6-address* } [**udp-port** *port*] command in global configuration mode to send logs to a specified log server.

Configuring the Level of Logs Sent to the Log Server

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

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

Configuring the Facility Value of Logs Sent to the Log Server

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

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

Configuring the Source Address of Logs Sent to the Log Server

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

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

Run the **logging source** { **ip** *ip-address* | **IPv6** *IPv6-address* } command to configure the source IP address of logs. If this IP address is not configured on the device, the source address of logs is the IP address of the interface sending logs.

Writing Logs into Log Files

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

Run the { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* | **sd0**:*filename* } 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 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.

1.3.4 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.

1.3.5 Featured Logging

The featured logging functions include level-based logging, delayed logging, and periodical logging. If the RFC5424 log format is enabled, logs can be sent in all directions, delayed logging is enabled, and periodical logging is disabled by default. If the RFC5424 log format is disabled, level-based logging, delayed logging, and periodical logging are disabled.

Working Principle

↘ Level-based Logging

You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure commands to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

↘ Delayed Logging

After generated, logs are not directly sent to the log server, and instead they are buffered in the log file. The device sends the log file to the syslog server through FTP at a certain interval. This function is called delayed logging.

If the device generates too many logs, sending all logs to the server in real time may deteriorate the performance of the device and the syslog server, and increase the burden of the network. In this case, the delayed logging function can be used to reduce the packet interaction.

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. By default, the file name prefix is syslog_ftp_server, the delayed logging interval is 3600s (one hour), and the log file size is 128 KB.

The maximum value of the delayed logging interval is 65535s, that is, 18 hours. If you set the delayed logging interval to the maximum value, the amount of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, logs will be written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period will be sent to the FTP or TFTP server at a time.

The Flash on the device that is used to buffer the local log files is limited in size. A maximum of eight log files can be buffered on the device. If the number of local log files exceeds eight before the timer expires, all log files that are generated earlier will be sent to the FTP or TFTP server at a time.

↘ Periodical Logging

Logs about performance statistics are periodically sent. All periodical logging timers are managed by the syslog module. When the timer expires, the syslog module calls the log processing function registered with each module

to output the performance statistic logs and send logs in real time to the remote syslog server. The server analyzes these logs to evaluate the device performance.

By default, the periodical logging interval is 15 minutes. To enable the server to collect all performance statistic logs at a time, you need to set the log periodical logging intervals of different statistic objects to a common multiple of them. Currently, the interval can be set to 0, 15, 30, 60, or 120. 0 indicates that periodical logging is disabled.

Related Configuration

Configuring the Level-based Logging Policy

By default, device logs are sent in all directions.

Run the **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** } command in global configuration mode to configure the level-based logging policy.

Enabling Delayed Display of Logs on the Console and Remote Terminal

By default, delayed display of logs on the Console and remote terminal is disabled.

Run the **logging delay-send terminal** command in global configuration mode to enable delayed display of logs on the Console and remote terminal.

Configuring the Name of the File for Delayed Logging

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. The default file name prefix is syslog_ftp_server.

Run the **logging delay-send file flash:***filename* command in global configuration mode to configure the name of the log file that is buffered on the local device.

Configuring the Delayed Logging Interval

By default, the delayed logging interval is 3600s (one hour).

Run the **logging delay-send interval** *seconds* command in global configuration mode to configure the delayed logging interval.

Configuring the Server Address and Delayed Logging Mode

By default, logs are not sent to any FTP or TFTP server.

Run the **logging delay-send server** { *ip-address* | **IPv6** *IPv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** } command in global configuration mode to configure the server address and delayed logging mode.

Enabling Periodical Logging

By default, periodical logging is disabled.

Run the **logging statistic enable** command in global configuration mode to enable periodical uploading of logs. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

Enabling Periodical Display of Logs on the Console and Remote Terminal

By default, periodical display of logs on the Console and remote terminal is disabled.

Run the **logging statistic terminal** command in global configuration mode to enable periodical display of logs on the Console and remote terminal.

Configuring the Periodical Logging Interval

By default, the periodical logging interval is 15 minutes.

Run the **logging statistic mnemonic** *mnemonic* **interval** *minutes* command in global configuration mode to configure the periodical logging interval.

1.3.6 Syslog Monitoring

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

Working Principle

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

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

Related Configuration

Enabling Logging of Login or Exit Attempts

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

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

Enabling Logging of Operations

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

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

1.4 Configuration

Configuration	Description and Command	
Configuring Syslog Format	⚠ (Optional) It is used to configure the syslog format.	
	service timestamps [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]	Configures the timestamp format of syslogs.

Configuration	Description and Command	
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
	service log-format rfc5424	Enables the RFC5424 syslog format.
Sending Syslogs to the Console	⚠ (Optional) It is used to configure parameters for sending syslogs to the Console.	
	logging on	Enables logging.
	logging count	Enables log statistics.
	logging console [*level*]	Configures the level of logs displayed on the Console.
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	⚠ (Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [*level*]	Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	⚠ (Optional) It is used to configure parameters for writing syslogs into the memory buffer.	
	logging buffered [*buffer-size*] [*level*]	Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log Server	⚠ (Optional) It is used to configure parameters for sending syslogs to the log server.	
	logging server { *ip-address* | **IPv6** *IPv6-address* } [**udp-port** *port*]	Sends logs to a specified log server.
	logging trap [*level*]	Configures the level of logs sent to the log server.
	logging facility *facility-type*	Configures the facility value of logs sent to the log server.
	logging source [**interface**] *interface-type interface-number*	Configures the source interface of logs sent to the log server.
	logging source { **ip** *ip-address* | **IPv6** *IPv6-address* }	Configures the source address of logs sent to the log server.
	logging trap [*level*]	Configures the level of logs sent to the log server.

Configuration	Description and Command	
	logging facility *facility-type*	Configures the facility value of logs sent to the log server.
Writing Syslogs into Log Files	(Optional) It is used to configure parameters for writing syslogs into a file.	
	logging file { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* | **sd0**:*filename* } [*max-file-size*] [*level*]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging flash interval *seconds*	Configures the interval at which logs are written into log files. The default value is 3600.
	logging life-time level *level days*	Configures the storage time of log files.
Configuring Syslog Filtering	(Optional) It is used to enable the syslog filtering function.	
	logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }	Configures the log filtering direction.
	logging filter type { **contains-only** | **filter-only** }	Configures the log filtering mode.
	logging filter rule exact-match module *module-name* **mnemonic** *mnemonic-name* **level** *level*	Configures the exact-match filtering rule.
	logging filter rule single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }	Configures the single-match filtering rule.
Configuring Level-based Logging	(Optional) It is used to configure logging policies to send the syslogs based on module and severity level .	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	Sends logs to different destinations by module and severity level
Configuring Delayed Logging	(Optional) It is used to enable the delayed logging function.	
	logging delay-send terminal	Enables delayed display of logs on the Console and remote terminal.
	logging delay-send file flash:*filename*	Configures the name of the file on the local device where logs are buffered.
	logging delay-send interval *seconds*	Configures the interval at which logs are sent to the log server.
	logging delay-send server { *ip-address* | **IPv6** *IPv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }	Configures the server address and delayed logging mode.
	(Optional) It is used to enable the periodical logging function.	

Configuration	Description and Command	
Configuring Periodical Logging	**logging statistic enable**	Enables the periodical logging function .
	logging statistic terminal	Enables periodical display of logs on the Console and remote terminal.
	logging statistic mnemonic *mnemonic* **interval** *minutes*	Configures the interval at which logs of a performance statistic object are sent to the server .
Configuring Syslog Monitoring	⚠ (Optional) It is used to configure parameters of the syslog monitoring function .	
	logging userinfo	Enables logging of login/exit attempts.
	logging userinfo command-log	Enables logging of operations.
Synchronizing User Input with Log Output	⚠ (Optional) It is used to configure the synchronization of user input and log output.	
	logging synchronous	Configures the synchronization of user input and log output.

1.4.1 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.

Adding a Space Next to the <pri> Option in the Log Format

- (Optional) By default, no space is added next to the <pri> option in the log format.
- Unless otherwise specified, you should perform this configuration on the device that needs a space next to the <pri> option in the log format.

Verification

- Generate a syslog, and check the log format.

Related Commands

Configuring the Timestamp Format of Syslogs

Command	**service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]
Parameter Description	*message-type*: Indicates the log type. There are two log types: log and debug. **uptime**: Indicates the device startup time in the format of dd:hh:mm:ss, for example, 07:00:10:41. **datetime**: Indicates the current device time in the format of MM DD hh:mm:ss, for example, Jul 27 16:53:07. **msec**: Indicates that the current device time contains millisecond. **year**: Indicates that the current device time contains year.
Command Mode	Global configuration mode
Configuration Usage	Two syslog timestamp formats are available, namely, uptime and datetime. You can select a timestamp format as required.

Adding the Sysname to the Syslog

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

Adding the Sequence Number to the Syslog

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

Enabling the Standard Syslog Format

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

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

Enabling the Private Syslog Format

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

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

Enabling the RFC5424 Syslog Format

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

Configuration Example

Enabling the RFC3164 Log Format

Scenario	It is required to configure the timestamp format as follows: 1. Enable the RFC3164 format. 2. Change the timestamp format to datetime and add the millisecond and year to the timestamp. 3. Add the sysname to the log. 4. Add the sequence number to the log.
Configuration Steps	● Configure the syslog format.
	Hostname# configure terminal Hostname(config)# no service log-format rfc5424 Hostname(config)# service timestamps log datetime year msec Hostname(config)# service timestamps debug datetime year msec Hostname(config)# service sysname Hostname(config)# service sequence-numbers
Verification	After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format. ● Run the **show logging config** command to display the configuration.

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

Enabling the RFC5424 Log Format

Scenario	It is required to enable the RFC5424 format.
Configuration Steps	● Configure the syslog format.
	Hostname# configure terminal Hostname(config)# service log-format rfc5424
Verification	Verify that new syslogs are displayed in the RFC5424 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the new log.
	Hostname(config)#exit <133>1 2013-07-24T12:19:33.130290Z Hostname SYS 5 CONFIG - Configured from console by console Hostname#show logging config Syslog logging: enabled

	Console logging: level debugging, 4740 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 4745 messages logged Statistic log messages: disable Statistic log messages to terminal: disable Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds Count log messages: enable Trap logging: level informational, 2641 message lines logged,4155 fail logging to 192.168.23.89 logging to 2000::1 Delay-send logging: 2641 message lines logged logging to 192.168.23.89 by tftp

1.4.2 Sending Syslogs to the Console

Configuration Effect

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

Notes

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

Configuration Steps

↘ Enabling Logging

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

↘ Enabling Log Statistics

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

↘ Configuring the Level of Logs Displayed on the Console

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

↘ Configuring the Log Rate Limit

- (Optional) By default, the no rate limit is configured.

- Unless otherwise specified, perform this configuration on the device to limit the log rate.

Verification

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

Related Commands

Enabling Logging

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

Enabling Log Statistics

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

Configuring the Level of Logs Displayed on the Console

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

Configuring the Log Rate Limit

Command	**logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]
Parameter Description	*number*: Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000. **all**: Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7. **console**: Indicates the number of logs displayed on the Console per second.

	except *severity*: Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configuration Usage	By default, no rate limit is configured.

Configuration Example

Sending Syslogs to the Console

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configuration Steps	● Configure parameters for displaying syslogs on the Console.
	Hostname# configure terminal Hostname(config)# logging count Hostname(config)# logging console informational Hostname(config)# logging rate-limit console 50
Verification	● Run the **show logging config** command to display the configuration.
	Hostname(config)#show logging config Syslog logging: enabled Console logging: level informational, 1303 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 1303 messages logged File logging: level informational, 118 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 118 message lines logged,0 fail

1.4.3 Sending Syslogs to the Monitor Terminal

Configuration Effect

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

Notes

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

Configuration Steps

↘ Allowing the Monitor Terminal to Display Logs

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

↘ Configuring the Level of Logs Displayed on the Monitor Terminal

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

Verification

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

Related Commands

↘ Allowing the Monitor Terminal to Display Logs

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

↘ Configuring the Level of Logs Displayed on the Monitor Terminal

Command	**logging monitor** [*level*]
Parameter Description	*level*: Indicates the log level.

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

Configuration Example

↘ Sending Syslogs to the Monitor Terminal

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	● Configure parameters for displaying syslogs on the monitor terminal.
	Hostname# configure terminal Hostname(config)# logging monitor informational Hostname(config)# line vty 0 4 Hostname(config-line)# monitor
Verification	● Run the **show logging config** command to display the configuration.
	Hostname#show logging config 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.

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

Configuration Example

↘ Writing Syslogs into the Memory Buffer

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	● Configure parameters for writing syslogs into the memory buffer.
	Hostname# configure terminal Hostname(config)# logging buffered 131072 informational
Verification	● Run the **show logging config** command to display the configuration and recent syslogs.
	Hostname#show logging Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail Log Buffer (Total 131072 Bytes): have written 4200 001301: *Jun 14 2013 19:01:09.488: Hostname %SYS-5-CONFIG_I: Configured from console by admin on console 001302: *Jun 14 2013 19:01:40.293: Hostname %SYS-5-CONFIG_I: Configured from console by admin on console //Logs displayed are subject to the actual output of the **show logging** command.

1.4.5 Sending Syslogs to the Log Server

Configuration Effect

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

Notes

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

Configuration Steps

Sending Logs to a Specified Log Server

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

Configuring the Level of Logs Sent to the Log Server

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

Configuring the Facility Value of Logs Sent to the Log Server

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

Configuring the Source Interface of Logs Sent to the Log Server

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

Configuring the Source Address of Logs Sent to the Log Server

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

Verification

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

Related Commands

Sending Logs to a Specified Log Server

Command	**logging server** { *ip-address* | **IPv6** *IPv6-address* } [**udp-port** *port*]
Parameter Description	*ip-address*: Specifies the IP address of the host that receives logs. **IPv6** *IPv6-address*: Specifies the IPv6 address of the host that receives logs. **udp-port** *port*: Specifies the port ID of the log server. The default port ID is 514.
Command Mode	Global configuration mode

Configuration Usage	This command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs will be sent simultaneously to all these log servers. You can configure up to five log servers on a device product.

Configuring the Level of Logs Sent to the Log Server

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

Configuring the Facility Value of Logs Sent to the Log Server

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

Configuring the Source Interface of Logs Sent to the Log Server

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

Configuring the Source Address of Logs Sent to the Log Server

Command	**logging source** { **ip** *ip-address* | **IPv6** *IPv6-address* }
Parameter Description	**ip** *ip-address*: Specifies the source IPv4 address of logs sent to the IPv4 log server. **IPv6** *IPv6-address*: Specifies the source IPv6 address of logs sent to the IPv6 log server.
Command Mode	Global configuration mode
Configuration Usage	By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs.

	To facilitate management, you can use this command to set the source IP address of all logs to the IP address of an interface so that the administrator can identify the device that sends the logs based on the unique address.

Configuration Example

↘ Sending Syslogs to the Log Server

Scenario	It is required to configure the function of sending syslogs to the log server as follows: 1. Set the IPv4 address of the log server to 10.1.1.100. 2. Set the source interface to Loopback 0. 3. Set the logs that cannot be received. Send the logs of IP assignment by DHCP to the log server. 4. Set the warning (Level 4) logs that can be sent to the log server.
Configuration Steps	● Configure parameters for sending syslogs to the log server.
	Hostname# configure terminal Hostname(config)# logging server 10.1.1.100 Hostname(config)# logging source interface Loopback 0
Verification	● Run the **show run | inc logging server** command to display the parameter configuration. ● Run the **show logging config** command to display the configuration.
	Hostname#show run | inc logging server logging server 10.1.1.100 Hostname#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level informational, 122 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100

1.4.6 Writing Syslogs into Log Files

Configuration Effect

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

Notes

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

Configuration Steps

↘ Writing Logs into Log Files

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

↘ Configuring the Number of Log Files

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

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

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

↘ Configuring the Storage Time of Log Files

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

↘ Immediately Writing Logs in the Buffer into Log Files

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

Verification

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

Related Commands

↘ Writing Logs into Log Files

Command	**logging file** { **sata0:***filename* | **flash:***filename* | **flash2:***filename* | **usb0**:*filename* | **usb1**:*filename* | **sd0**:*filename* } [*max-file-size*] [*level*]
Description	**sata0**: Indicates that log files are stored on the hard disk drive. **flash**: Indicates that log files are stored on the extended Flash. **flash2**: Indicates that log files are stored on the extended FLASH2. **usb0**: Indicates that log files will be stored on USB 0. This option is supported only when the device has one USB port and a USB flash drive is inserted into the USB port. **usb1**: Indicates that log files will be stored on USB 1. This option is supported only when the device has two USB ports and USB flash drives are inserted into the USB ports. **sd0**: Indicates that log files will be stored on the SD card. This option is supported only when the device has an SD port and an SD card is inserted into the SD port. *filename*: Indicates the log file name, which does not contain a file name extension. The file name extension is always txt. *max-file-size*: Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default value is 128 KB. *level*: Indicates the level of logs that can be written into a log file.
Command Mode	Global configuration mode
Configuration Usage	This command is used to create a log file with the specified file name on the specified file storage device. The file size increases with the amount of logs, but cannot exceed the configured maximum size. If not specified, the maximum size of a log file is 128 KB by default. After this command is configured, the system saves logs to log files. A log file name does not contain any file name extension. The file name extension is always txt, which cannot be changed. After this command is configured, logs will be written into log files every hour. If you run the **logging flie flash:syslog** command, a total of 16 log files will be created, namely, **syslog.txt**, **syslog_1.txt**, **syslog_2.txt**, ..., **syslog_14.txt**, and **syslog_15.txt**. Logs are written into the 16 log files in sequence. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is full. When **syslog_15.txt** is full, logs are written into **syslog.txt** again. If no extended flash space is available, the **logging file flash** command is automatically hidden and cannot configured. If no FLASH2 is available, the **logging file flash2** command is hidden automatically and cannot be configured. Otherwise, the logs are stored in FLASH2 after the **logging file flash** command is configured.

Configuring the Interval at Which Logs Are Written into Log Files

Command	**logging flash interval** *seconds*
Parameter Description	*seconds*: Indicates the interval at which logs are written into log files. The value ranges from 1s 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** *level days*

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

Immediately Writing Logs in the Buffer into Log Files

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

Configuration Example

Writing Syslogs into Log Files

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.
	Hostname# configure terminal Hostname(config)# logging file flash:syslog debugging Hostname(config)# logging flash interval 600
Verification	● Run the **show logging config** command to display the configuration.
	Hostname(config)#show logging config

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

1.4.7 Configuring Syslog Filtering

Configuration Effect

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

Notes

- Two filtering modes are available: contains-only and filter-only. You can configure only one filtering mode at a time.
- If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Configuration Steps

Configuring the Log Filtering Direction

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

Configuring the Log Filtering Mode

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

Configuring the Log Filtering Rule

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

Verification

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

Related Commands

Configuring the Log Filtering Direction

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

Configuring the Log Filtering Mode

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

Configuring the Log Filtering Rule

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

Configuration Example

↘ Configuring Syslog Filtering

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

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

1.4.8 Configuring Level-based Logging

Configuration Effect

- You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure a command to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

Notes

- Level-based logging takes effect only when the RFC5424 format is enabled.

Configuration Steps

↘ Configuring Level-based Logging

- (Optional) By default, logs are sent in all directions.
- Unless otherwise specified, perform this configuration on the device to configure logging polices to send syslogs to different destinations based on module and severity level.

Verification

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

Related Commands

↘ Configuring Level-based Logging

Command	**logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }
Parameter Description	*module-name*: Indicates the name of the module to which the logging policy is applied. **not-lesser-than**: If this option is specified, logs of the specified level or higher will be sent to the specified destination, and other logs will be filtered out. If this option is not specified, logs of the specified level or lower will be sent to the specified destination, and other logs will be filtered out. *level*: Indicates the level of logs for which the logging policy is configured. **all**: Indicates that the logging policy is applied to all logs. **server**: Indicates that the logging policy is applied only to logs sent to the log server. **file**: Indicates that the logging policy is applied only to logs written into log files. **console**: Indicates that the logging policy is applied only to logs sent to the Console. **monitor**: Indicates that the logging policy is applied only to logs sent to a remote terminal. **buffer**: Indicates that the logging policy is applied only to logs stored in the buffer.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure logging polices to send syslogs to different destinations based on module and severity level.

Configuration Example

Configuring Level-based Logging

Scenario	It is required to configure the logging policies as follows: 1. Send logs of Level 5 or higher that are generated by the system to the Console. 2. Send logs of Level 3 or lower that are generated by the system to the buffer.
Configuration Steps	● Configure the logging policies.
	Hostname# configure terminal Hostname(config)# logging policy module SYS not-lesser-than 5 direction console Hostname(config)# logging policy module SYS 3 direction buffer
Verification	● Run the **show running-config | include logging policy** command to display the configuration. ● Exit and enter global configuration mode to generate a log containing module name “SYS”. Verify that the log is sent to the destination as configured.
	Hostname#show running-config | include logging policy logging policy module SYS not-lesser-than 5 direction console logging policy module SYS 3 direction buffer

1.4.9 Configuring Delayed Logging

Configuration Effect

- By default, delayed logging is enabled by default at the interval of 3600s (one hour). The name of the log file sent to the remote server is ***File size_Device IP address_Index*.txt**. Logs are not sent to the Console or remote terminal.
- You can configure the interval based on the frequency that the device generates logs for delayed uploading. This can reduce the burden on the device, syslog server, and network. In addition, you can configure the name of the log file as required.

Notes

- This function takes effect only when the RFC5424 format is enabled.
- It is recommended to disable the delayed display of logs on the Console and remote terminal. Otherwise, a large amount of logs will be displayed, increasing the burden on the device.
- The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5.The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.
- If few logs are generated, you can set the interval to a large value so that many logs can be sent to the remote server at a time.

Configuration Steps

↘ Enabling Delayed Display of Logs on Console and Remote Terminal

- (Optional) By default, delayed display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable delayed display of logs on the Console and remote terminal.

↘ Configuring the Name of the File for Delayed Logging

- (Optional) By default, the name of the file for delayed logging is ***File size_Device IP address_Index*.txt**.
- Unless otherwise specified, perform this configuration on the device to configure the name of the file for delayed logging.

↘ Configuring the Delayed Logging Interval

- (Optional) By default, the delayed logging interval is 3600s (one hour).

- Unless otherwise specified, perform this configuration on the device to configure the delayed logging interval.

Configuring the Server Address and Delayed Logging Mode

- (Optional) By default, log files are not sent to any remote server.
- Unless otherwise specified, perform this configuration on the device to configure the server address and delayed logging mode

Verification

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

Related Commands

Enabling Delayed Display of Logs on Console and Remote Terminal

Command	**logging delay-send terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A.

Configuring the Name of the File for Delayed Logging

Command	**logging delay-send file flash:***filename*
Parameter Description	**flash:***filename*: Indicates the name of the file on the local device where logs are buffered.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the name of the file on the local device where logs are buffered. The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the configured file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.

Configuring the Delayed Logging Interval

Command	**logging delay-send interval** *seconds*
Parameter Description	*seconds*: Indicates the delayed logging interval. The unit is second.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the delayed logging interval. The value ranges from 600s to 65,535s.

Configuring the Server Address and Delayed Logging Mode

Command	**logging delay-send server** { *ip-address* | **IPv6** *IPv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }
Parameter Description	*ip-address*: Indicates the IP address of the server that receives logs. **IPv6** *IPv6-address*: Indicates the IPv6 address of the server that receives logs. *username*: Specifies the user name of the FTP server. *password*: Specifies the password of the FTP server. **0**: (Optional) Indicates that the following password is in plain text. **7**: Indicates that the following password is encrypted.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify an FTP or a TFTP server for receiving the device logs. You can configure a total of five FTP or TFTP servers, but a server cannot be both an FTP and TFTP server. Logs will be simultaneously sent to all FTP or TFTP servers.

Configuration Example

Configuring Delayed Logging

Scenario	It is required to configure the delayed logging function as follows: 1. Enable the delayed display of logs on the Console and remote terminal. 2. Set the delayed logging interval to 7200s (two hours). 3. Set the name of the file for delayed logging to syslog_Hostname. 4. Set the IP address of the server to 192.168.23.12, user name to admin, password to admin, and logging mode to FTP.
Configuration Steps	● Configure the delayed logging function.
	Hostname# configure terminal Hostname(config)# logging delay-send terminal Hostname(config)# logging delay-send interval 7200 Hostname(config)# logging delay-send file flash:syslog_Hostname Hostname(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
Verification	● Run the **show running-config | include logging delay-send** command to display the configuration. ● Verify that logs are sent to the remote FTP server after the timer expires.
	Hostname#show running-config | include logging delay-send logging delay-send terminal logging delay-send interval 7200 logging delay-send file flash:syslog_Hostname logging delay-send server 192.168.23.12 mode ftp user admin password admin

1.4.10 Configuring Periodical Logging

Configuration Effect

- By default, periodical logging is disabled. Periodical logging interval is 15 minutes. Periodical display of logs on the Console and remote terminal are disabled.
- You can modify the periodical logging interval. The server will collect all performance statistic logs at the time point that is the least common multiple of the intervals of all statistic objects.

Notes

- Periodical logging takes effect only when the RFC5424 format is enabled.
- The settings of the periodical logging interval and the function of displaying logs on the Console and remote terminal take effect only when the periodical logging function is enabled.
- It is recommended to disable periodical display of logs on the Console and remote terminal. Otherwise, a large amount of performance statistic logs will be displayed, increasing the burden on the device.

- To ensure the server can collect all performance statistic logs at the same time point, the timer will be restarted when you modify the periodical logging interval of a statistic object.

Configuration Steps

Enabling Periodical Logging

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

Enabling Periodical Display of Logs on Console and Remote Terminal

- (Optional) By default, periodical display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical display of logs on the Console and remote terminal.

Configuring the Periodical Logging Interval

- (Optional) By default, the periodical logging interval is 15 minutes.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs of statistic objects are sent to the server.

Verification

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

Related Commands

Enabling Periodical Logging

Command	**logging statistic enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to enable periodical logging. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

Enabling Periodical Display of Logs on Console and Remote Terminal

Command	**logging statistic terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Periodical Logging Interval

Command	**logging statistic mnemonic** *mnemonic* **interval** *minutes*
Parameter Description	*mnemonic*: Identifies a performance statistic object. *minutes*: Indicates the periodical logging interval. The unit is minute.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the periodical logging interval for a specified performance statistic object. The interval can be set to 0, 15, 30, 60, or 120 minutes. 0 indicates that periodical logging is disabled.

Configuration Example

Configuring Periodical Logging

Scenario	It is required to configure the l periodical logging function as follows: 1. Enable the periodical logging function. 2. Enable periodical display of logs on the Console and remote terminal. 3. Set the periodical logging interval of the statistic object TUNNEL_STAT to 30 minutes.
Configuration Steps	● Configure the periodical logging function.
	Hostname# configure terminal Hostname(config)# logging statistic enable Hostname(config)# logging statistic terminal Hostname(config)# logging statistic mnemonic TUNNEL_STAT interval 30
Verification	● Run the **show running-config | include logging statistic** command to display the configuration. ● After the periodical logging timer expires, verify that logs of all performance statistic objects are generated at the time point that is the least common multiple of the intervals of all statistic objects.
	Hostname#show running-config | include logging statistic logging statistic enable logging statistic terminal logging statistic mnemonic TUNNEL_STAT interval 30

1.4.11 Configuring Syslog Monitoring

Configuration Effect

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

- Record modification of device configurations. After logging of operations is enabled, the related logs are displayed on the device when users modify the device configurations. This helps the administrator monitor the changes in device configurations.

Notes

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

Configuration Steps

Enabling Logging of Login/Exit Attempts

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

Enabling logging of Operations

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

Verification

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

Related Commands

Enabling Logging of Login/Exit Attempts

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

Enabling Logging of Operations

Command	**logging userinfo command-log**
Parameter Description	N/A
Command Mode	Global configuration mode

Configuration Usage	The system generates related logs when users run configuration commands. By default, a device generates logs when users modify device configurations.

Configuration Example

Configuring Syslog Monitoring

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

1.4.12 Synchronizing User Input with Log Output

Configuration Effect

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

Notes

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

Configuration Steps

Synchronizing User Input with Log Output

- (Optional) By default, the synchronization function is disabled.

- Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

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

Related Commands

Synchronizing User Input with Log Output

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

Configuration Example

Synchronizing User Input with Log Output

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

1.5 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**

1 Configuring Software Upgrade

1.1 Overview

Package management (pkg_mgmt) is a package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying and maintaining various components of the device, among which upgrade is the main function. Through upgrade, users can install new version of software that is more stable or powerful. Adopting a modular structure, the RGOS system not only supports overall upgrade and subsystem upgrade but also supports separate upgrade of a feature package.

Component upgrade described in this document applies to both the box-type device and rack-type device. In addition, this document is for only version 11.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

1.2 Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem firmware like boot, kernel, and rootfs on the device.
Upgrading/Degrading a Single Feature Package	Upgrade a single feature package on the device.

1.2.1 Upgrading/Degrading Subsystem

Scenario

After the upgrade of a subsystem firmware is complete, all system software on the device is updated, and the overall software is enhanced. Generally, the subsystem firmware is called main package.

The main features of this upgrade mode are as follows: All software on the device is updated after the upgrade is completed; all known software bugs are fixed. It takes a long time to finish upgrade.

Deployment

You can store the main package in the root directory of the TFTP server, download the package to the device, and then run an upgrade command to upgrade the package locally. You can also store the main package in a USB flash drive or SD card, connect the USB flash drive SD card to the device, and then run an upgrade command to upgrade the package.

1.2.2 Upgrading/Degrading a Single Feature Package

Scenario

Device software consists of several components, and each component is an independent feature module. After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced with the other features unchanged.

The features of this upgrade mode are as follows: Generally, a feature package is small and the upgrade speed is high. After the upgrade is completed, only the corresponding functional module is improved, and other functional modules remain unchanged.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive or SD card, connect the USB flash drive to the device, and then complete the upgrade.

1.3 Features

Basic Concepts

Subsystem

A subsystem exists on a device in the form of images. Include:

- boot: After being powered on, the device loads and runs the boot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.
- kernel: kernel is the OS core part of the system. This subsystem shields hardware composition of the system and provides applications with abstract running environment.
- rootfs: rootfs is the collection of applications in the system.

Main Package

- Main package is often used to upgrade/degrade a subsystem of the box-type device. The main package is a combination package of the boot, kernel, and rootfs subsystems. The main package can be used for overall system upgrade/degradation.

Feature Package

- The feature package refers to a collection which enables a certain feature. When the device is delivered, all supported functions are contained in the rootfs subsystem. You can upgrade only a specific feature by upgrading a single feature package.

Hot Patch Package

- A hot patch package contains the hot patches of multiple features. You can upgrade the hot patch package to install the patches for each feature package in sequence. In this way, new features are immediately available without restarting the device.

"Firmware" in this document refers to an installation file that contains a subsystem or feature module.

Overview

Feature	Description

Upgrading/Degrading and Managing Subsystem Components	Upgrades/degrades a subsystem and checks available subsystem components.
Upgrading/Degrading and Managing Functional Components	Upgrades/degrades a functional component, checks available subsystem components, and activate the specified subsystem component.

1.3.1 Upgrading/Degrading and Managing Subsystem Components

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystem components of the device with the subsystem components in the firmware. The subsystem component contains redundancy design. Subsystems of the device are not directly replaced with the subsystems in the package during upgrade/degradation in most cases. Instead, subsystems are added to the device and then activated during upgrade/degradation.

Working Principle

↘ Upgrade/Degradation

Various subsystems exist on the device in different forms. Therefore, upgrade/degradation varies with different subsystems.

- boot: Generally, this subsystem exists on the norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.
- kernel: This subsystem exists in a specific partition in the form of files. Therefore, upgrading/degrading this subsystem is to write the file.
- rootfs: Generally, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the nandflash device.

↘ Management

Query the subsystem components that are available currently and then load subsystem components as required.

Each subsystem component contains redundancy design. During the upgrade/degradation:

- boot: The boot subsystem always contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is involved in the upgrade, and the slave boot subsystem serves as the redundancy backup all along.
- kernel: as the kernel subsystem contains at least one redundancy backup. More redundancy backups are allowed if there is enough space.
- rootfs: The rootfs subsystem always contains a redundancy backup.

The boot component is not included in the scope of subsystem management due to its particularity. During upgrade of the kernel or rootfs subsystem component, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem component, and management information about various versions.

Relevant Configuration

↘ Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

1.3.2 Upgrading/Degrading and Managing Functional Components

Working Principle

In fact, upgrading a feature is replacing feature files on the device with the feature files in the package.

Managing feature components is aimed at recording the information of feature components by using a database. In fact, installing, displaying and uninstalling a component is the result of performing the Add, Query and Delete operation on the database.

After package upgrade, component upgrade cannot be performed.

Relevant Configuration

↘ Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

1.4 Configuration

Configuration	Description and Command	
Upgrading/Degrading a Firmware	⚠ The basic function of the configuration is installing and upgrading/degrading a subsystem firmware, feature package.	
	upgrade download tftp://*path* ***[force]****url*	*pathurl* refers to a local path where a installation package file is stored. This command is used to download an installation package from the server and upgrade the firmware stored on the device.
	upgrade rollbackdownload tftp://*path*	*path* refers to a path of an installation package on the server. This command is used to download an installation package from the server and upgrade the package automatically.

1.4.1 Upgrading/Degrading a Firmware

Configuration Effect

Available upgrade packages include the following types:

- After the upgrade of the main package is complete, all system software on the line card is updated, and the overall software is enhanced.

- After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced, with other features remain unchanged.
- A hot patch package is installed to fix software bugs without restarting the device. It is used to upgrade a specific version of software only.

Generally a main package is released to upgrade a box-type device.

Notes

N/A

Configuration Steps

Upgrading the Main Package for a Single Device

- Optional configuration. This configuration is required when all system software on the device needs to be upgraded.
- Download the firmware to the local device and run the **upgrade** command.

Generally a main package is pushed to upgrade a box-type device.

Upgrading Each Feature Package

- Optional configuration. The configuration is used to fix bugs of a certain feature and enhance the function of this feature.
- Download the firmware to the local device and run the **upgrade** command.

Subsystem Rollback

- Optional configuration. This configuration aims to roll a subsystem back to the state before the upgrade, select this configuration item.
- This configuration takes effect after you run the **upgrade** command to upgrade the subsystem component (for example, the main package or the rack package).

After you run the **upgrade** command to upgrade a subsystem component in the user scenario, you can run the rollback command once, that is, consecutive rollback is not supported.

Upgrading the Server

- Optional. This function is enabled by default. You can use the configuration to disable the server.
- After the server is disabled, automatic upgrade cannot be performed if no line card with the main program is inserted. If an upgrade package of a line card is being downloaded from the server, the server cannot be disabled.

Verification

- After upgrading a subsystem component, you can run the **show upgrade history** command to check whether the upgrade is successful.
- After upgrading a feature component, you can run the **show component** command to check whether the upgrade is successful.

Commands

Upgrade

Command	**upgrade download tftp://***path* [**force**]
Parameter Description	*path*: Indicates the path of the upgrade package.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Firmware Stored on the Device

Command	**show upgrade file** *url*
Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Subsystem Component Rollback

Command	**upgrade rollback**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to undo the last subsystem upgrade operation and make the subsystem restore to the state before the upgrade. You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.

Displaying the Feature Components Already Installed

Command	**show component** [*component _name*]
Parameter Description	[*component _name*]: component name When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Patch Package Already Installed

Command	**show patch** [*patch_name*]

Parameter Description	*patch_name*: Indicates the name of the patch package file.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Example of Upgrading a Subsystem Firmware on the Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive or SD card, insert the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive or SD card.
Configuration Steps	● Run the upgrade command. ● After upgrading the subsystem, restart the device.
	Hostname# upgrade download tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin... !!! !!! !!! !!! !!!!!!!!!!!!!!!!! Transmission finished, file length 21525888 bytes. Upgrade processing is 10% Upgrade processing is 60% Upgrade processing is 90% Upgrade info [OK] Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f] Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8] Upgrade processing is 100% Reload system to take effect! Reload system?(Y/N)y Restarting system.
Verification	● Check the system version on the current device. If the version information changes, the upgrade is successful.
	Hostname#show version detail

	System description : EG1000m System start time : 2013-10-19 02:25:28 System uptime : 0:00:00:50 System hardware version : 1.00 System software version : RGOS11.0(1C2) Release(20131022) System boot version : 1.0.0.e7a1451 System core version : 2.6.32.9f8b56f System main version : 1.0.0.1bcc12e8 System boot build : unknown System core build : 2013/10/22 04:54:03 System main build : 2013/10/22 05:33:38

Example of Upgrading a Feature Package on the Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive or SD card, connect the USB flash drive or SD card to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the **upgrade** command. ● Check whether the device needs to be restarted based on the prompt displayed after the upgrade.
	Hostname#upgrade sata0://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm Hostname#upgrade sata0://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm Upgrade processing is 10% Upgrade processing is 60% Upgrade processing is 90% Upgrade info [OK] bridge version[2.0.1.37cd5cda ->2.3.1.1252ea] [OK] Upgrade processing is 100% Reload system to take effect! Reload system?(Y/N)y Restarting system.
Verification	● Check the version of the feature component on the current device. If the version information changes, the upgrade is successful.
	Hostname#show version detail System description : Hostname AP820-L(V2) (802.11a/n/ac/ax and 802.11b/g/n/ax) By Ruijie Networks.

	System start time : 1970-02-07 00:33:24 System uptime : 0:00:47:28 System hardware version : 2.00 System software version : RGOS 11.0(5)B1 System patch number : NA System software number : M01181304092015 System serial number : 1234942570019 System boot version : 1.2.9.f23dcbe(150317) System core version : 2.6.32.6b31161115502c

Example of Subsystem Rollback on the Device

You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive or SD card, connect the USB flash drive or SD card to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the subsystem rollback command. ● Restart the device for the rollback to take effect.
	Hostname#upgrade rollback kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK] rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK] Rollback success! Reload system to take effect! Reload system?(Y/N)y Restarting system.
Verification	● Check the system version on the current device. If t it is restored to the version before the upgrade, the rollback is successful.
	Hostname#show version System description : Hostname AP820-L(V2) (802.11a/n/ac/ax and 802.11b/g/n/ax) By Ruijie Networks. System start time : 2022-09-01 16:58:32 System uptime : 0:00:22:09 System hardware version : 1.00 System software version : AP_RGOS 11.9(6)W1B1, Release(09192519) System patch number : NA System serial number : G1PH649000094 System boot version : 2017.09

Common Errors

If an error occurs during the upgrade, the upgrade module displays an error message. The following provides an example:

```
Upgrade info [ERR]
        Reason:creat config file err(217)
```

The following describes several types of common error messages:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. It is recommended to obtain the firmware again and perform the upgrade operation.
- Firmware not supported by the device: The cause is that you may use the firmware of other devices by mistake. It is recommended to obtain the firmware again, verify the package, and perform the upgrade operation.
- Insufficient device space: Generally, this error occurs on a rack-type device. It is recommended to check whether the device is supplied with a USB flash drive or SD card. Generally, this device has a USB flash drive.

1.5 Monitoring

Clearing

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

Description	Command
Removes an installation package on the local device.	**clear storage** [*url*]

Displaying

Description	Command
Displays all components already installed on the current device and their information.	**show component** [*component _name*]

1 Configuring Time Range

1.1 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.

1.2 Typical Application

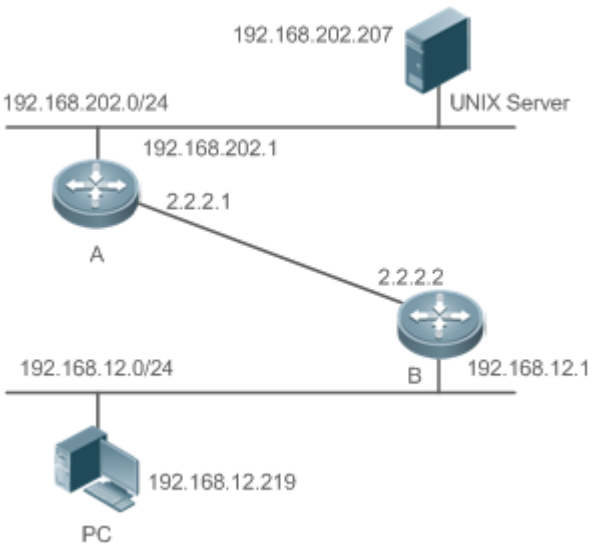
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

1.2.1 Applying Time Range to an ACL

Application Scenario

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

Figure 1-1



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

Functional Deployment

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

1.3 Function Details

Basic Concepts

Absolute Time Range

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

Periodic Time

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

Features

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

1.3.1 Using Absolute Time Range

Working Principle

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

1.3.2 Using Periodic Time

Working Principle

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

1.4 Configuration Details

Configuration Item	Suggestions and Related Commands

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

1.4.1 Configuring Time Range

Configuration Effect

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

Configuration Method

Configuring Time Range

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

Command	**time-range** *time-range-name*
Parameter Description	*time-range-name*: name of the time range to be created.
Defaults	No time range is configured by default.
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

- Optional configuration.

Command	**absolute** { [**star**t *time date*] | [**end** *time date*] }
Parameter Description	**star**t *time date*: start time of the range. **end** *time date*: end time of the range.
Defaults	No absolute time range is configured. The default is the maximum time range.
Command Mode	Time range configuration mode
Usage Guide	Use the **absolute** command to configure an 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

- Optional configuration.

Command	**periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*
Parameter Description	*day-of-the-week*: the week day when the periodic time starts or ends *time*: the exact time when the periodic time starts or ends
Defaults	No periodic time is configured. By default, it is within the periodic time.
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.

Verification

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

Command	**show time-range** [*time-range-name*]
Parameter Description	*time-range-name*: specifies a time range to be displayed.
Command Mode	Privileged EXEC mode
Usage Guide	Use the **show time-range** [*time-range-name*] command to check the time range configuration.
Verification	1：Display the time range configuration: Hostname# show time-range time-range entry: test (inactive) absolute end 01:02 02 February 2012

1.5 Monitoring and Maintaining Time Range

Displaying

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

Configuring Interface

1. Configuring Ethernet Interface
2. Configuring Aggregated Port

1 Configuring Ethernet Interface

1.1 Overview

Interfaces are important parts for data exchange on network devices. Devices support two types of interfaces: physical interfaces and logical interfaces. A physical interface is a real entity that exists on a device, for example, GigabitEthernet (GE) interface. A logical interface is a virtual interface that does not actually exist on a device. A logical interface can be associated with or independent of a physical interface, for example, a loopback or tunnel interface. In network protocols, physical and logical interfaces are treated equally.

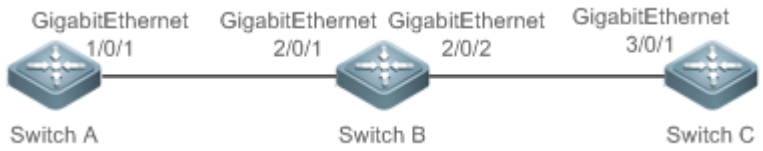
1.2 Applications

Application	Description
Route-based Layer 3 Communication Through Ethernet Physical Interfaces	Layer-3 data communication is implemented on network devices through a Layer 3 Ethernet physical interface.

1.2.1 Route-based Layer 3 Communication Through Ethernet Physical Interfaces

Scenario

Figure 1-1



As shown in the preceding figure, Switch A, Switch B, and Switch C form a simple Layer 3 data communication network.

Deployment

- Connect Switch A to Switch B through physical interfaces GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical interfaces GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as Layer 3 routed ports.
- Set the IP addresses of GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1 respectively to 192.168.1.1/24 and 192.168.1.2/24 which are in the same network segment.
- Set the IP addresses of GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1 respectively to 192.168.2.1/24 and 192.168.2.2/24 which are in the same network segment.

- Configure a static route on Switch C so that Switch C can directly go through the 192.168.1.0/24 network segment on layer 3. Configure a static route on Switch A so that Switch A can directly go through the 192.168.2.0/24 network segment on layer 3.
- Run ping 192.168.2.2 and ping 192.168.1.1 respectively on Switch A and Switch C to enable Layer 3 routing on Switch B.

1.3 Features

Basic Concepts

Interface Types

Interfaces on devices are classified into two categories:

- Layer 2 interface (switch or bridge mode)
- Layer 3 interface (supported by Layer 3 devices)

1. Common Layer 2 interfaces are classified into the following types:

- Switch port
- Layer 2 aggregate interface

2. Common Layer 3 interfaces are classified into the following types:

- Routed port
- Layer 3 aggregate interface
- Switch virtual interface (SVI)
- Loopback interface
- Tunnel interface

Switch port

A switch port consists of a single physical interface on the device and provides only the Layer 2 switching function. Switch ports are used to manage physical interfaces and their associated Layer 2 protocols.

Layer 2 aggregate interface

An aggregate interface is formed by binding multiple physical member interfaces. Several physical links can be bound together to form a logical link, which is called an aggregate interface.
For Layer 2 switching, an aggregate interface acts like a high-bandwidth switch port. The Layer 2 interface can combine the bandwidths of multiple ports to expand link bandwidth. In addition, frames sent through a Layer 2 aggregate interface are load balanced on member ports of the Layer 2 aggregate interface. If one member link of the aggregate interface fails, the Layer 2 aggregate interface automatically switches traffic on this link to other available member links, improving connection reliability.

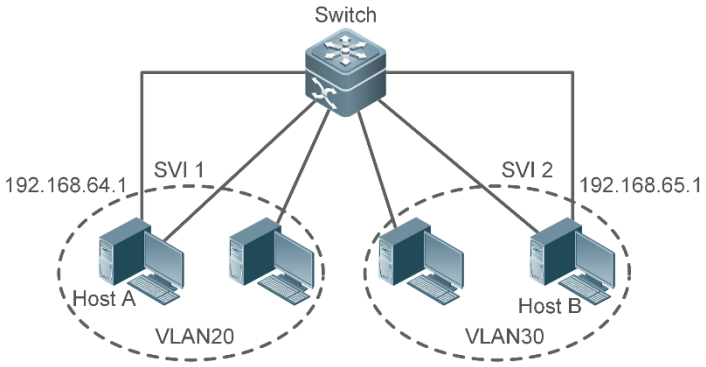
SVI

An SVI can be used as the management interface of the local device. Administrators can manage a device through the SVI. You can also create an SVI as a gateway interface, which is mapped to the virtual interface of each virtual

local area network (VLAN) to implement routing across VLANs among Layer 3 devices. You can run the **interface vlan** command to create an SVI and assign an IP address to this interface to realize communication between VLANs.

As shown in Figure1-3, hosts in VLAN 20 can directly communicate with each other without Layer 3 devices. If Host A in VLAN 20 attempts to communicate with Host B in VLAN 30, SVI 1 of VLAN 20 and SVI 2 of VLAN 30 must be used.

Figure 1-1



Routed port

- On Layer 3 devices, you can configure a physical interface as a routed port and use it as the gateway interface for Layer 3 switching. A routed port is irrelevant to a specific VLAN. Instead, it just serves as an access port. Routed ports do not support the Layer 2 switching function.

You can run the **no switchport** command to switch a switch port to a routed port and assign an IP address to this routed port to realize communication. Note that all Layer 2 features of the switch port will be deleted after you run the **no switchport** command.

If a port is a member port of a Layer 2 aggregate interface or 802.1X authentication fails to be performed on the port, you cannot run the **switchport** or **no switchport** command to configure the switch port or routed port.

Layer 3 aggregate interface

Like a Layer 2 aggregate interface, a Layer 3 aggregate interface is formed by binding multiple physical member interfaces. The interface is to be aggregated must be Layer 3 interfaces of the same type. An aggregate interface serves as the gateway interface for Layer 3 switching. It treats multiple physical links in the same aggregate group as one logical link. It is an important way to expand link bandwidth. In addition, frames sent through a Layer 3 aggregate interface are load balanced on member ports of the Layer 2 aggregate interface. If one member link of the aggregate interface fails, the Layer 3 aggregate interface automatically switches traffic on this link to other available member links, improving connection reliability.

Layer 3 aggregate interfaces do not support the Layer 2 switching function. You can run the **no switchport** command to switch a Layer 2 aggregate interface without any member port into a Layer 3 aggregate interface, add multiple routed ports to the Layer 3 aggregate interface, and then assign an IP address to the Layer 3 aggregate interface to realize communication.

- Loopback Interface

The loopback interface is a local Layer 3 logical interface simulated by software. The interface is always up. Packets sent to the loopback interface are processed on the device locally, including routing information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) protocol, or as the

destination IP address of the Telnet server or the source IP address of the Telnet client. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface. You can treat the loopback interface as a virtual Ethernet interface.

Tunnel Interface

A tunnel interface implements the tunnel function by using transmission protocols (such as IP) to transmit packets under any protocol. Same as other logical interfaces, a tunnel interface is also a virtual system interface. Instead of particularly specifying any transmission protocol or load protocol, a tunnel interface provides a standard point-to-point transmission mode. Since that, a tunnel interface must be set for each individual link.

Overview

Feature	Description
Configuring Interfaces	You can configure interface attributes in interface configuration mode. If the interface to be configured is a logical interface which does not exist, create the interface after the interface configuration mode is entered.
Configuring the Interface Description and Status	You can name an interface for identification of the interface features. You can set the status of an interface.
Configuring the MTU	You can set the Maximum Transmission Unit (MTU) for an interface to control the maximum size of the frames received or sent on this interface.
Configuring the Bandwidth	You can configure the interface bandwidth in interface configuration mode.
Configuring the Load Calculation Interval	You can specify the time interval of calculating the loads of packet input/output.
Configuring the Carrier Delay	You can modify the acceptable carrier delay of an interface within which the link status switching from Down to Up or from Up to Down.
Link Trap Policy	The device can decide whether to send link trap information of the interface based on interface configuration.
Interface Index Persistence	Enable the interface index persistence function. That is, the interface index remains unchanged after the device is restarted.
Interface Rate and Duplex	Configure the rate and duplex mode of an interface.
Port Flapping Protection	Configure the port flapping protection function. The system can automatically shut down the port when flapping occurs on the port.
Interface Syslog	Enable the Syslog function on an interface. The system will display prompts if an exception occurs on the interface.
Configuring VLAN Tag Encapsulation on Interfaces	You can configure 802.1Q encapsulation on an interface. When sending a packet, the interface adds a VLAN ID to the packet header. When receiving a packet, the interface removes the VLAN ID from the packet header.

1.3.1 Configuring Interfaces

Run the **interface** command in global configuration mode to enter the interface configuration mode. In interface configuration mode, you can configure interface attributes.

Working Principle

Run the **interface** command in global configuration mode to enter the interface configuration mode. If the interface to be configured is a logical interface which does not exist, the interface will be created after the interface configuration mode is enabled. You can also run the **interface range** or **interface range macro** command in global configuration mode to configure interfaces (interface IDs) within a specific range. The interfaces within one 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 logical interface or logical interfaces within a specific range.

Interface Numbering Rules

In standalone mode, the interface ID of a physical interface consists of two parts: slot number and interface number in the slot. For example, if the slot number is 2 and the interface number in the slot is 3, the interface ID is 2/3. In VSU mode or stacking mode, the interface ID of a physical interface consists of three parts: device number, slot number, and interface number in the slot. For example, if the device number is 1, the slot number is 2, and the interface number in the slot is 3, the interface ID is 1/2/3.

The device number ranges from 1 to the maximum number of supported member devices.

Slot numbering rule: The number of a fixed slot is 0 while that of a dynamic slot (swappable module or line card) ranges from 1 to the number of slots. For dynamic slots, face the device panel to sequence the slots from front to back, left to right, and up to down, with the slot number increasing from 1.

The interface number in the slot ranges from 1 to the number of interfaces in the slot, increasing one by one from left to right.

On the devices where medium types can be select, you can select the 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 aggregate interface ranges from 1 to the maximum number of aggregate interfaces supported by the device.

The ID of an SVI is the VID of the VLAN corresponding to the SVI.

Configuring Interfaces Within a Specific Range

You can run the **interface range** command in global configuration mode to configure multiple interfaces at the same time. The attributes you set under this command apply to all interfaces within the range you have selected.

Specify interfaces within a certain range.

The **interface range** command can be used to specify multiple interface ranges.

The **macro** parameter can be specified using the macro of a range. For details, see "Configuring the Interface Macro".

Ranges can be separated by commas (,).

The types of interfaces of all ranges specified in one command must be the same.

Pay attention to the format of the **range** parameter when you run the **interface range** command.

The following common interface range formats are valid:

- **FastEtherne**t device/slot/{first port} - {last port};

- **GigabitEthernet** device/slot/{first interface} - {last interface}
- **TenGigabitEthernet** device/slot/{first port} - {last port};
- **FortyGigabitEthernet** device/slot/{first port} - {last port};
- **AggregatePort** Aggregate-port ID-Aggregate-port ID (The ID ranges from 1 to the maximum number of aggregate interfaces supported by the device.)
- **vlan** vlan-ID-vlan-ID (The VLAN ID ranges from 1 to 4,094.)
- **Loopback loopback** loopback-ID - loopback-ID (The loopback ID ranges from 1 to 2,147,483,647.)
- **Tunnel** tunnel-ID - tunnel-ID (The tunnel ID ranges from 0 to the maximum number of tunnel interfaces supported by the device minus 1)
- Interfaces within one **interface range** must be of the same type. That is, all of them are GigabitEthernet or FastEthernet.

Configuring the Interface Macro

You can define macros to avoid manually entering interface ranges. Before using the **macro** keyword in the **interface range** command, you need to run the **define interface-range** command to define these macros in global configuration mode.

Run the **no define interface-range** *macro_name* command in global configuration mode to delete the configured macros.

1.3.2 Configuring the Interface Description and Status

You can name an interface for identification of the interface features.

You can enable or disable an interface in interface configuration mode.

Working Principle

Interface Description

You can name an interface based on the purpose it is used for. For example, if you want to assign GigabitEthernet 1/1 to user A, you can describe this interface as "Port for User A".

Interface Status

An interface has two states: Up and Down. If an interface is disabled, it is in Down state; otherwise, it is in Up state. In certain cases, you may need to disable an interface. You can directly disable an interface by setting the status of the interface. If an interface is disabled, the interface will not receive or send any frames, indicating that all its features are lost. You can also re-enable a disabled interface by setting the status of the interface.

1.3.3 Configuring the MTU

You can set the MTU for an interface to control the maximum size of the frames received or sent on this interface.

On some devices the MTU cannot be configured on an interface but can be configured globally.

Working Principle

When exchanging a great throughput of data, an interface may receive jumbo frames whose size is larger than that of typical Ethernet frames. MTU is the size of a valid data segment of a frame. It does not include the overhead of Ethernet encapsulation.

If the size of a frame received or forwarded by an interface exceeds the specified MTU, the frame will be discarded.

1.3.4 Configuring the Bandwidth

Working Principle

The **bandwidth** command is used forrouting protocols (for example, OSPF) to calculate the route metrics and for Resource Reservation Protocol (RSVP) to calculate the retained bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of a physical interface.

Running this command does not affect the fixed bandwidth of an interface at the physical layer, which functions as a routing factor.

1.3.5 Configuring the Load Calculation Interval

Working Principle

The **load-interval** command can be used to set the interval of calculating packet input/output. Usually the interval is set to 10 seconds.

1.3.6 Configuring the Carrier Delay

Working Principle

The carrier delay refers to the acceptable time delay in status change of the Data Carrier Detect (DCD) signal from Down to Up or from Up to Down. If the DCD status changes within the delay, the system will ignore this change and the upper data link layer does not need to renegotiate. If the carrier delay is set to a large value, nearly every transient DCD change will be ignored. On the contrary, if the parameter is set to **0**, every DCD signal change however minor will be detected by the system, resulting in higher instability.

If the DCD carrier interrupts for a long time, set the parameter to a smaller value to accelerate topology convergence and route summarization. On the contrary, if the period of DCD carrier interruption is smaller than the time of topology convergence or route summarization, set the parameter to a larger value to avoid topology or route flapping.

1.3.7 Link Trap Policy

You can enable or disable the link trap function on an interface based on the interface configuration.

Principles

When the link trap function on an interface is enabled, the device enabled with Simple Network Management Protocol (SNMP) sends link trap messages when the link status changes on the interface.

1.3.8 Interface Index Persistence

Like an interface name, an interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. Enable the interface index persistence function. The interface index remains unchanged after the device is restarted.

Principles

After the interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.3.9 Interface Rate and Duplex

You can configure the rate and duplex of an Ethernet physical interface or aggregate interface.

Principles

↘ Interface Rate

Typically, the rate of an Ethernet physical interface is determined through auto-negotiation with the peer device. The negotiated rate can be any rate within the interface capability. You can also configure any rate within the interface capability for the Ethernet physical interface.

When you configure the rate of an aggregate interface, the configuration takes effect on all of its member interfaces. All these member interfaces are Ethernet physical interfaces.

↘ Duplex Mode

- The duplex mode of an Ethernet physical interface or aggregate interface 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 aggregate interface, the configuration takes effect on all of its member interfaces. All these member interfaces are Ethernet physical interfaces.

1.3.10 Port Flapping Protection

A port flap causes a lot of hardware interruptions, consuming many CPU resources. Moreover, frequent port flapping damages the port. You can configure the port flapping protection function to protect ports.

Principles

By default, the port flapping protection function is enabled. You can disable this function as required. When a port flap occurs, the port detects flapping every 2s or 10s. If the port detect six flaps in 2s, the device displays a prompt. If the device display 10 prompts continuously, that is, the port detects flapping continuously within 20s, the port is shut down (the cause is displayed as **Link Dither**). If the port detects 10 flaps within 10s on a port, the device displays a prompt without shutting down the port.

1.3.11 Interface Syslog

You can enable or disable the Syslog function to determine whether to view information about interface status changes or exceptions.

Principles

You can enable or disable the Syslog function as required. By default, this function is enabled. When an exception occurs on an interface, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

1.3.12 Configuring VLAN Tag Encapsulation on Interfaces

Working Principle

A virtual LAN (VLAN), namely a logical network partitioned in a physical network, is a layer-2 network of the OSI model. IEEE issued the 802.1Q protocol standard in 1999 to standardize VLAN implementation.

The VLAN technology allows a network administrator to partition a physical LAN into different broadcast areas (or VLANs) logically. Each VLAN consists of a group of computer workstations with the same needs. Therefore, they have the same features as the physical LAN. However, since VLANs are partitioned logically but not physically, the workstations in a VLAN do not need to be placed in the same physical space. In other words, these workstations do not necessarily belong to the same physical LAN network segment. The broadcast and unicast traffic on a VLAN cannot be forwarded to other VLANs, which helps control traffic, reduces equipment investment, simplifies network management, and improves network security.

VLAN is a protocol proposed to solve the Ethernet broadcast problem and security issues. On the basis of an Ethernet frame, a VLAN header is added and a VLAN ID is used to assign users into smaller work groups to restrict the mutual access at Layer 2 between different work groups. Each work group is a VLAN. The advantage of a VLAN is to restrict the broadcasting scope, build virtual work groups, and dynamically manage networks.

To communicate with a host in a VLAN, you can configure the 802.1Q (VLAN protocol) VLAN encapsulation tag on an Ethernet interface or sub interface. In this way, the Ethernet interface encapsulates the VLAN header when sending a packet and detaches the VLAN header when receiving a packet.

Related Configuration

↘ **Configuring the 802.1Q VLAN Tag**

By default, the 802.1Q encapsulation protocol is disabled for interfaces.

You can run the **encapsulation dot1Q** *VLAN-ID* command in interface configuration mode to encapsulate 802.1Q on an interface. *VLAN-ID* is the VLAN ID to be encapsulated.

1.4 Configuration

Configuration	Description and Command	
Configuring Interfaces	⚠ (Optional) It is used to create, delete, and describe an interface.	
	interface	Creates an interface and enters the interface configuration mode of this interface, or directly enters the interface configuration mode of an interface.
	interface range	Configures interfaces within a specific range. If no interface is created, this command can be used to create and configure interfaces in batches.
	define interface-range	Defines the interface macro for batch operation.
	snmp-server if-index persist	Enables interface index persistence. That is, an interface index remains the same after the device is restarted.
	description	Describes an interface in interface configuration mode with a maximum of 80 characters.
	snmp trap link-status	Enables link trap on an interface in interface configuration mode.
	shutdown	Disables an interface in interface configuration mode.
	physical-port dither protect	Configures the port flapping protection function in global configuration mode.
	logging [**link-updown** | **error-frame** | **link-dither** | **res-lack-frame**]	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 interface bandwidth in interface configuration mode.
	carrier-delay	Configures the carrier delay of an interface in interface configuration mode.
	load-interval	Configures the load calculation interval of an interface in interface configuration mode.
	duplex	Configures the duplex mode of an interface.
	mtu	Configures the MTU of an interface.

Configuration	Description and Command	
	speed	Configures the interface rate.
	encapsulation dot1Q	Configures the 802.1Q VLAN tag on an interface.

1.4.1 Configuring Interfaces

Configuration Effect

- Create a specified logical interface and enter the interface configuration mode. For an existing physical or logical interface, directly enter the interface configuration mode.
- Create specified logical interfaces in batches and enter the interface configuration mode. For an existing physical or logical interface, directly enter the interface configuration mode.
- Enable interface index persistence so that the interface index remains the same after the device is restarted.
- Configure the interface description to intuitively and vividly describe an interface.
- Enable or disable link trap on an interface.
- Configure the interface status by enabling or disabling the interface.

Notes

- You can run the **no** form of this command to delete a specified logical interface or logical interfaces in a specified range, but cannot run the **no** form of this command to delete a physical interface or physical interfaces in a specified range.
- You can run the **default** form of this command in interface configuration mode to restore default settings of a specified physical interface or a logical interface, or interfaces in a specified range.

Configuration Steps

↘ Configuring an Interface

- Optional.
- This command is used to create a non-existing logical interface or configure an existing physical or logical interface in interface configuration mode.

Command	**interface** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: indicates the type and ID of the interface. The interface can be an Ethernet physical interface, aggregate interface, SVI, or loopback interface.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	• If a logical interface is not created, run this command to create a logical interface and enter the configuration mode of the interface. • For a physical interface or an existing logical interface, run this command to enter the configuration mode of the interface. • Run the **no** form of this command to delete a specified logical interface.

	• Run the **default** form of this command to restore default settings of the interface in interface configuration mode.

Configuring Interfaces Within a Specific Range

- Optional.
- To create non-existing logical interfaces in batches or configure multiple existing physical or logical interfaces in interface configuration mode, run this command.

Command	**interface range** { *port-range* | **macro** *macro_name* }
Parameter Description	*port-range*: indicates the type and ID range of interfaces. The interfaces can be Ethernet physical interfaces, aggregate interfaces, SVIs, or loopback interfaces. *macro_name*: indicates the macro name of interface types in a range.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	• If logical interfaces are not created , run this command to create logical interfaces and enter the batch configuration mode of the interface. • For multiple physical interfaces or existing logical interfaces, run this command to enter the batch configuration mode of the interfaces. • Run the **default** form of this command to restore default settings of the interfaces in interface configuration mode in batches. • Before using a macro, run the **define interface-range** command to define the interface types in a range as a macro name in global configuration mode. Then run the **interface range macro** macro_name command to apply the macro.

Enabling Interface Index Persistence

- Optional.
- This command is used in a scenario where the interface indexes must remain unchanged after the device is restarted.

Command	**snmp-server if-index persist**
Parameter Description	N/A
Defaults	This function is disabled.
Command Mode	Global configuration mode
Usage Guide	After this command is executed, current indexes of all interfaces are saved, and the interface indexes remain unchanged after the device is restarted. You can run the **no** or **default** form of this command to disable the interface index persistence function.

Configuring the Interface Description

- Optional.
- Run this command to configure the description of an interface.

Command	**description** *string*
Parameter Description	*string*: Up to 80 characters
Defaults	By default, no description is configured on an interface.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the description string of an interface. Run the **no** or **default** form of this command to remove the description string of the interface. -

Enabling or Disabling Link Trap

- Optional.
- Run this command to obtain link trap messages of interface status changes through SNMP.

Command	**snmp trap link-status**
Parameter Description	-
Defaults	By default, the link trap function is enabled.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the link trap function on an interface. When this function is enabled, SNMP enables the device to send link traps when the link status changes on the interface. Run the **no** or **default** form of this command to disable the link trap function.

Configuring 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	The default administrative status of an interface is Up.
Command Mode	Interface configuration mode
Usage Guide	Run the **shutdown** command to disable an interface, or run the **no shutdown** command to enable the interface. Run the **no** or **default** form of this command to enable the interface. Depending on the product model, when the port is shut down, there are two possible cases: 1. You cannot run the **no shutdown** command on the port. 2. You can run the **shutdown** or **no shutdown** command to recover the errdisable port.

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	**link-updown**: logs status change information. **error-frame**: logs error frame information. **link-dither**: logs port flapping information.
Defaults	By default, the Syslog function is enabled on an interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Configuring an Interface

- If you can enter the interface configuration mode after running the **interface** command, 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 interface has been properly deleted.
- After running the **default interface** command on an interface, you can run the **show running** command to check whether the configurations under the interface are restored to the default values. If so, the configuration is successful.

Configuring Interfaces Within a Specific Range

- If you can properly enter the interface configuration mode after running the **interface range** command, the configuration is successful.
- After running the **default interface** command for an interface, you can run the **show running** command to check whether the configurations under the interface are restored to the default values. If so, the configuration is successful.

Enabling Interface Index Persistence

- After running the snmp-server if-index persist command, run write to save the configuration. Then restart the device and run the show interface command to display the interface index. If the interface index remains the same after the device is restarted, the configuration is successful.

Enabling or Disabling Link Trap

- Select a physical interface, plug or remove the network cable, and then start the SNMP server. If the SNMP server can properly receive the traps about link status changes of an interface, the function is enabled properly.
- After running the no form of this command, select a physical interface, plug or remove the network cable, and then start the SNMP server. If the SNMP server cannot receive the traps about link status changes of this interface, link trap has been properly disabled.

Configuring the Interface Status

- Select a physical interface, install the network cable to make the interface Up, and run the shutdown command to disable this interface. If the Syslog information on the console shows that the interface status changes to Down and the LED of this interface turns off, the interface is properly disabled. Run the **show interfaces** command. The port status is displayed as administratively down. Then run the no shutdown command to restart this interface. If the Syslog information on the Console shows that the interface status changes to Up and the LED of this interface turns on, the interface is properly re-enabled.

Configuring Port Flapping Protection

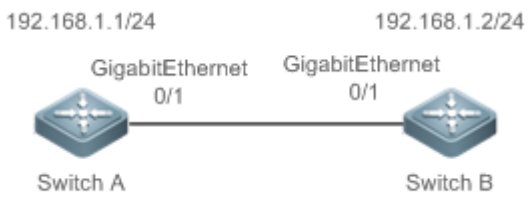
- Run the **physical-port dither protect** command in global configuration mode. Frequently remove and insert the network cable on a physical port to simulate port flapping. Verify that a syslog indicating port flapping is displayed on the Console. After such a syslog is displayed for several times, the system prompts that the port will be shutdown.
- Run the **physical-port dither period** command in global configuration mode to enable flapping detection. You can define violating ports by configuring detection period duration, threshold for flapping and the number of consecutive violating period.

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 Interface Attributes

Scenario Figure 1-4	
Configuration Steps	• Connect two switches through their switch ports.

	● Configure an SVI on each of the two switches, and assign IP addresses in the same network segment to the two SVIs. ● Enable the interface index persistence function on the two switches. ● Enable the link trap function on the two switches. ● Configure interface status on the two switches.
A	A# configure terminal A(config)# snmp-server if-index persist A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# snmp trap link-status A(config-if-GigabitEthernet 0/1)# shutdown A(config-if-GigabitEthernet 0/1)# end A# write
B	B# configure terminal B(config)# snmp-server if-index persist B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface gigabitethernet 0/1 B(config-if-GigabitEthernet 0/1)# snmp trap link-status B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write
Verification	Perform the following operations on Switch A and Switch B respectively: ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether the status of GigabitEthern 0/1 and SVI 1 is correct. ● After running the **shutdown** command, check whether GigabitEthernet 0/1 sends traps when the link status of this interface changes to Down. ● After the device is restarted, check whether the interface index of GigabitEthernet 0/1 remains the same.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is administratively down , line protocol is DOWN Hardware is GigabitEthernet, address is 00d0.f865.de9b0a (bia 00d0.f865.de9b0a) Interface address is: no ip address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255

	Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0 Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second Priority is 0 admin medium-type is Copper, oper medium-type is Copper admin duplex mode is AUTO, oper duplex is Unknown admin speed is AUTO, oper speed is Unknown flow control admin status is OFF, flow control oper status is Unknown admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Port-type: access Vlan id: 1 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns , 0 dropped 0 output errors, 0 collisions, 0 interface resets A# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP , line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) Interface address is: 192.168.1.1/24 ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit

	Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is administratively down , line protocol is DOWN Hardware is GigabitEthernet Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b) MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0 Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second Priority is 0 admin medium-type is Copper, oper medium-type is Copper admin duplex mode is AUTO, oper duplex is Unknown admin speed is AUTO, oper speed is Unknown flow control admin status is OFF, flow control oper status is Unknown admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Port-type: access Vlan id: 1

	10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns , 0 dropped 0 output errors, 0 collisions, 0 interface resets B# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP , line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) Interface address is: 192.168.1.2/24 ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255

Common Errors

- N/A

1.4.2 Configuring Interface Attributes

Configuration Effect

- Enable the switch to connect and communicate with other devices through the switch port or routed port.
- Adjust interface attributes on devices.

Notes

- N/A

Configuration Steps

↘ Configuring the Interface Rate

- Optional.
- A port flap may occur if the configured speed of a port changes.
- This command is applicable to an Ethernet physical interface or aggregate interface.

Command	**speed** [**10** | **100** | **1000** | **auto**]
Parameter Description	**10**: The interface rate is10 Mbps. **100**: The interface rate is100 Mbps. **1000**: The interface rate is 1000 Mbps. **Auto**: The interface rate is determined through auto-negotiation.

Defaults	By default, the interface rate is determined through auto-negotiation. That is, the default mode of the interface rate is auto.
Command Mode	Interface Mode
Usage Guide	If an interface is a member interface of an aggregate interface, the rate of the interface is determined by the rate of the aggregate interface. When the member interface is deleted from the aggregate interface, the member interface uses its own rate configuration. Run the **show interfaces** command to display rate configurations. The rates available to an interface vary with the type of the interface. For example, you cannot set the rate of an SFP interface to 10 Mbps.

Configuring the Duplex Mode

- Optional.
- Port flapping may occur if the configured duplex mode of a port changes.
- This command is applicable to an Ethernet physical interface or aggregate interface.

Command	**duplex** { **auto** | **full** | **half** }
Parameter Description	**Auto**: Auto negotiation. **full**: Full duplex. **Half**: Half duplex.
Defaults	By default, the duplex mode of an interface is auto.
Command Mode	Interface Mode
Usage Guide	The duplex mode of an interface is related to the interface type. Run the **show interfaces** command to display duplex configurations of an interface.

Configuring the MTU

- Optional.
- Configure the MTU of a port to limit the length of a frame that can be received or sent over this port.
- This command is applicable to an Ethernet physical interface or SVI.

Command	**mtu** *num*
Parameter Description	*num*: 64 to 9,216
Defaults	By default, the MTU of an interface is 1,500 bytes.
Command Mode	Interface Mode
Usage Guide	Run this command to configure the interface MTU, that is, the maximum length of a data frame at the link layer. You can configure the MTU for only a physical interface or an aggregate interface with member interfaces.

Configuring the Bandwidth

- Optional.
- Generally, the interface bandwidth is the same as the interface rate.

Command	**bandwidth** *kilobits*
Parameter Description	*kilobits:* The value ranges from 1 to 2,147,483,647, in kbps.
Defaults	By default, the bandwidth of an interface matches the type of the interface. For example, the default bandwidth of a GE Ethernet physical interface is 1,000,000, and that of a 10GE Ethernet physical interface is 10,000,000.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Carrier Delay

- 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 {** *num* **}**
Parameter Description	*num*: The value ranges from 0 to 60, in seconds.
Defaults	The default carrier-delay time of an interface is 2s.
Command Mode	Interface configuration mode
Usage Guide	If carrier delay time is configured in milliseconds, the time must be an integer multiple of 100 milliseconds.

Configuring the Load Calculation Interval

- Optional.
- The configured load interval affects computation of the average packet rate on an interface. If the configured load interval is short, the average packet rate can accurately reflect the changes of the real-time traffic.

Command	**load-interval** *seconds*
Parameter Description	*seconds*: The value ranges from 5 to 600, in seconds.
Defaults	By default, the load interval of an interface is 10s.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring VLAN Tag Encapsulation on an Interface

- (Optional) If this function is required, run the encapsulation dot1Q command in interface configuration mode.
- The 802.1Q encapsulation protocol is disabled by default.

Command	encapsulation dot1Q VlanID

Parameter Description	VlanID: specifies the VLAN ID, in the range from 1 to 4,094.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Run the **show interfaces** command to display attribute configurations of interfaces.

Command	**show interfaces** [*interface-type interface-number*] [**description | switchport | trunk**]
Parameter Description	*interface-type interface-number*: indicates the type and number of the interface **description**: indicates the description of an interface, including the link status. **switchport**: indicates Layer 2 interface information. This parameter is valid only for a Layer 2 interface. **trunk**: indicates trunk port information. This parameter is valid for a physical interface or an aggregate interface.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command without any parameter to display basic interface information.
Command Presentation	SwitchA#show interfaces GigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is DOWN , line protocol is DOWN Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b) Interface address is: no ip address Interface IPv6 address is: No IPv6 address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Medium-type is Copper Admin duplex mode is AUTO, oper duplex is Unknown Admin speed is AUTO, oper speed is Unknown Flow receive control admin status is OFF,flow send control admin status is OFF Flow receive control oper status is Unknown,flow send control oper status is Unknown Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: Port-type: trunk Native vlan:1 Allowed vlan lists:1-4094 //The allowed VLAN list of the trunk port Active vlan lists:1, 3-4 // Effective VLANs (That is, only VLAN 1,VLAN 3, and VLAN 4 are created on the device.)

	Rxload is 1/255,Txload is 1/255 5 minutes input rate 0 bits/sec, 0 packets/sec 5 minutes output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 0 packets output, 0 bytes, 0 underruns , 0 dropped 0 output errors, 0 collisions, 0 interface resets

- Run the **show interfaces counters rate** command to display transmission rates of interfaces.

Command	**show interfaces counters rate** [**up** | **down**]
Parameter Description	**up**: displays transmission rates of interfaces in Up state. **down**: displays transmission rates of interfaces in Down state.
Command Mode	Privileged EXEC mode
Usage Guide	If the interface is not specified, the transmission rates of all physical interfaces and aggregate interfaces are displayed.
Command Presentation	Hostname#show interfaces counters rate up Interface Sampling Time Input Rate Input Rate Output Rate Output Rate (bits/sec) (packets/sec) (bits/sec) (packets/sec) ---------- ---------- ---------- ---------- ---------- ---------- Te1/21 5 seconds 0 0 762 0 Te1/22 5 seconds 0 0 212 0 Te1/23 5 seconds 511546 999 762 0 Te1/24 5 seconds 0 0 762 0 Te8/1 5 seconds 0 0 546946 1004 Ag4 5 seconds 0 0 834 0

Sampling Time	Sampling time.
Input Rate	Receiving rate
Output Rate	Sending Rate

- Run the **show interfaces brief** command to display brief interface information.

Command	**show interfaces** [*interface-type interface-number*] **brief** [**up** | **down**]
Parameter Description	*interface-type interface-number*: displays information of the specified interface. **up**: displays transmission rates of interfaces in Up state. The parameter is available only when no interface is specified.

	down: displays transmission rates of interfaces in Down state. The parameter is available only when no interface is specified.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display brief information of all physical and aggregate interfaces, including the link status, output and input bandwidth usage, and the number of error packets sent and received by interfaces.

1. Display the brief information about TenGigabitEthernet 0/1.

```
Hostname#show interfaces TenGigabitEthernet 0/1 brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface   Link Stat    Protocol Stat    Input Usage      Output Usage     inErrors    outErrors
--------    ---------    --------------   --------------   -------------    ----------  ----------
Te0/1       disabled     down             0.00%            0.00%            0           0
```

Link Stat	Link state
Protocol Stat	Protocol status
InputUsage	Input bandwidth usage
OutputUsage	Output bandwidth usage
inErrors	Number of error packets received by the interface
outErrors	Number of error packets sent by the interface

2. Display brief information about all connected interfaces.

```
Hostname#show interfaces brief up
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface   Link Stat    Protocol Stat    Input Usage      Output Usage     inErrors    outErrors
--------    ---------    --------------   --------------   -------------    ----------  ----------
Te0/1       up           up               78.20%           83.40%           0           0
Te0/2       up           up               73.40%           82.00%           0           0
```

3. Display brief information about all interfaces.

```
Hostname#show interfaces brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface   Link Stat    Protocol Stat    Input Usage      Output Usage     inErrors    outErrors
```

	-------- --------- --------------- --------------- ------------- ---------- ---------- Te0/1 down down 0.00% 0.00% 0 0 Te0/2 down down 0.00% 0.00% 0 0 Te0/3 down down 0.00% 0.00% 0 0 Te0/4 down down 0.00% 0.00% 0 0 Te0/5 down down 0.00% 0.00% 0 0 Te0/6 down down 0.00% 0.00% 0 0 Te0/7 down down 0.00% 0.00% 0 0 Te0/8 down down 0.00% 0.00% 0 0 Te0/9 down down 0.00% 0.00% 0 0 Te0/10 disabled down 0.00% 0.00% 0 0

- Run the **show interfaces brief** command to display Ethernet information about interfaces.

Command	**show interfaces** [*interface-type interface-number*] **ethernet brief [up | down]**
Parameter Description	*interface-type interface-number*: displays Ethernet information about the specified interface. **up**: Displays Ethernet information of interfaces in Up state. The parameter is available only when no interface is specified. **down**: Displays Ethernet information of interfaces in Down state. The parameter is available only when no interface is specified.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display brief information about all physical and aggregate interfaces, including the link status, VLANs, auto-negotiation mode, duplex mode, interface rates and bandwidth usage, and description (alias).
	1. Display brief information about GigabitEthernet 0/1. Hostname#show interfaces GigabitEthernet 0/1 brief down: link down *down: administratively down disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.) Interface Link Stat Vlan Auto-Neg Duplex Speed Input Usage Output Usage Description --------- --------- ---- -------- ------- ------- ----------- ------------- ----------- Gi0/1 down 1 OFF Unknown Unknown 0.00% 0.00% 10G port

Link Stat	Link status
Vlan	VLAN

Auto-Neg	Auto-negotiation mode
Duplex	Duplex mode
Speed	Interface rate
InputUsage	Input bandwidth usage
OutputUsage	Output bandwidth usage
Description	Description (alias)

2. Display brief information about all connected interfaces.

```
Hostname#show interfaces ethernet brief up
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface   Link Stat   Vlan   Auto-Neg   Duplex   Speed   Input Usage   Output Usage   Description
---------   ---------   ----   --------   -------  -------  -----------  -------------  -----------
Gi0/1       UP          1      OFF        Full     1000M    79.77%       79.77%         10G port
```

3. Display brief information about all interfaces.

```
Hostname#show interfaces ethernet brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface   Link Stat   Vlan   Auto-Neg   Duplex   Speed   Input Usage   Output Usage   Description
---------   ---------   ----   --------   -------  -------  -----------  -------------  -----------
Gi0/1       *down       1      OFF        Unknown  Unknown  0.00%        0.00%          10G port
Gi0/2       down        1      OFF        Unknown  Unknown  0.00%        0.00%
Gi0/3       down        1      OFF        Unknown  Unknown  0.00%        0.00%
Ag1         up          1      OFF        Full     1000M    46.78%       46.77%
Mg0         up          routed --         Full     1000M    --           --             IP management Console
```

Common Errors

N/A

1.5 Monitoring

Clearing

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

Description	Command
Clears the interface counters.	**clear counters** [*interface-type interface-number*]
Restarts an interface.	**clear interface** *interface-type interface-number*

Displaying

Displaying Interface Configuration and Status

Description	Command
Displays the status and configuration of an interface.	**show interfaces** [*interface-type interface-number*]
Displays the interface status.	**show interfaces** [*interface-type interface-number*] **status**
Displays interface errdisable status.	**show interfaces** [*interface-type interface-number*] **status err-disable**
Displays the time and times of link status changes.	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Displays the description and status of an interface.	**show interfaces** [*interface-type interface-number*] **description** [**up | down**]
Displays the counters of an interface, among which the rate may have an error within 0.5%.	**show interfaces** [*interface-type interface-number*] **counters** [**up | down**]
Displays the counters of packets increased in the previous sampling interval.	**show interfaces** [*interface-type interface-number*] **counters increment** [**up | down**]
Displays the error counters on an interface.	**show interfaces** [*interface-type interface-number*] **counters error** [**up | down**]
Displays the Tx/Rx rate of an interface.	**show interfaces** [*interface-type interface-number*] **counters rate** [**up | down**]
Displays the counter summary of an interface.	**show interfaces** [*interface-type interface-number*] **counters summary** [**up | down**]
Displays statistics on discarded packets on an interface. Displays the bandwidth usage of an interface.	**show interfaces** [*interface-type interface-number*] **counters drops** [**up | down**]**usage**
Displays the bandwidth usage of an interface.	**show interfaces** [*interface-type interface-number*] **usage** [**up | down**]
Displays brief information about all physical and aggregate interfaces, including link status, VLANs, auto-negotiation mode, duplex mode, interface rates and bandwidth usage, and description (alias).	show ip interface [interface-typeinterface-number | brief]

Description	Command
Displays VLAN sub-interface information.	**show vlans**

1 Configuring Aggregated Port

1.1 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

1.2 Applications

N/A

1.3 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.

↘ 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.

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.
Wireless AP Aggregated Port	The wireless AP achieves dual uplink deployment through link aggregation to improve reliability.

1.3.1 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.

1.3.2 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

Load balancing based on IP addresses or port numbers is applicable only to Layer-3 packets. When a device enabled with this load balancing method receives Layer-2 packets, it automatically switches to the default load balancing method.

All the load balancing methods use a load algorithm (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.

Different products may support different load balancing algorithms.

Enhanced Load Balancing

Enhanced load balancing allows the combination of multiple fields in different types of packets. These fields include **src-mac**, **dst-mac**, **l2-protocol**, **vlan**, **src-port**, and **dst-port** in Layer-2 packets, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **vlan**, **src-port**, **dst-port**, **l2-etype**, **src-mac**, and **dst-mac** in IPv4 packets, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **vlan**, **src-port**, **dst-port**, **l2-etype**, **src-mac**, and **dst-mac** in IPv6 packets; **top-label**, **2nd-label**, **3rd-label**, **src-ip**, **dst-ip**, **vlan**, **src-port**, **dst-port**, **src-mac**, **dst-mac**, **protocol**, **l4-src-port**,

l4-dst-port, and **l2-etype** in MPLS packets; **vlan**, **src-port**, **src-mac**, **src-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **l2-etype**, **ing-nick**, **egr-nick**, **dst-port**, **dst-mac**, and **dst-ip** in TRILL packets and **vlan**, **src-port**, **src-id**, **rx-id**, **ox-id**, **fabric-id**, **dst-port**, and **dst-id** in FCoE packets.

A device enabled with enhanced load balancing first determines the type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

- All the load balancing methods are applicable to Layer-2 and Layer-3 AP ports. You need to configure proper load distribution methods based on different network environments to fully utilize network bandwidth.
- Perform enhanced load balancing based on the src-mac, dst-mac, and vlan fields in Layer-2 packets, and the src-ip field in IPv4 packets. If the incoming packet is an IPv4 packet with an ever-changing source MAC address, the enhanced balancing algorithm does not take effect, because the device will perform load balancing only based on the src-ip field in the IPv4 packet after finding that it is an IPv4 packet.
- In enhanced load balancing, the MPLS balancing algorithm takes effect only for MPLS Layer-3 VPN packets, but does not take effect for MPLS Layer-2 VPN packets.

Hash Load Balancing Control

Hash load balancing enables users to control load balancing flexibly in different scenarios. Currently, Ruijie adopts the following hash load balancing control functions:

- Hash disturbance factor: Traffic over AP ports is hashed for balancing. For two devices of the same type, the same path will be calculated for load balancing for the same stream. When the ECMP is deployed, the same stream of the two devices may be balanced to the same destination device, resulting in hash polarization. The hash disturbance factor is used to affect the load balancing algorithm. Different disturbance factors are configured for different devices to ensure that different paths are provided for the same stream.
- Hash synchronization: To ensure network security, a firewall cluster is deployed between the internal and external networks for traffic cleaning. This requires that both the uplink and downlink traffic of a session is transmitted to the same device in the firewall cluster for processing. The source and destination IP addresses contained in the uplink and downlink streams of a session are reversed. The uplink and downlink streams will be directed to different firewalls in the firewall cluster based on the traditional hash algorithm. The hash synchronization function ensures that uplink and downlink streams of a session be transmitted over the same path.
- Flexible hash: In normal cases, the load balancing cluster interworks with multiple ToRs via the ECMP, and the ToRs are required to balance all packets of a session to the same scheduling server. However, when a server is faulty, all session streams will be ordered and balanced again based on the traditional load balancing mechanism of ToRs. In this case, packets of the same session may be balanced to two servers. The flexible hash function ensure that when one link is faulty, traffic on other links is not affected and only the traffic of the faulty link is balanced to other active links. In this case, traffic of a session will only be balanced to the same server.
- Hash algorithm mode: Apply the most appropriate hash algorithm mode to different traffic, so that when traffic changes, balance can still be kept. For example, if the source and destination MAC addresses of a stream increase 1 at the same time, configure the algorithm based on the source and destination MAC addresses cannot keep stream balance. At the moment, a suitable hash algorithm mode needs to be applied.

- Hash factor acquisition mode: There are an inner layer and an outer layer in the header in each of VXLAN packets, GRE packets, and other tunnel packets. It can be specified to obtain the hash factor from the inner layer or outer layer, to achieve a better balancing effect. For example, in some scenarios, tunnel packets share the same outer IP address but have different inner IP addresses. In this case, the inner IP address can be specified as the hash factor to optimize traffic balancing.

For different devices, the performance of hash algorithm mode may be different.

1.3.3 Wireless AP Aggregated Port

Working Principle

If the wireless traffic exceeds gigabit, a single wired port cannot meet the requirements. In this case, an aggregated port needs to be used for load balancing and bandwidth increasing. Wireless APs adopts the dual uplink deployment mode. If a network cable is disconnected, the other cable can continue to work, ensuring link backup. Aggregated port configuration of wireless APs is delivered by the AC or aggregated ports are configured independently on the APs. If wireless APs work in fit AP mode, aggregated port configuration is delivered by the AC. If wireless APs work in fat AP mode, aggregated ports are configured on the AP console over serial ports.

1.4 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.
Enabling LinkTrap	(Optional) It is used to enable LinkTrap.	
	snmp trap link-status	Enables LinkTrap advertisement for an AP port.
	aggregateport member linktrap	Enables LinkTrap t for AP member ports.
Configuring a Load Balancing Mode	(Optional) It is used to configure a load balancing mode for an aggregated link.	
	aggregateport load-balance	Configures a load balancing algorithm for an AP port or AP member ports.
	(Optional) It is used to configure the profile of enhanced load balancing.	

1.4.1 Configuring Static AP Ports

Configuration Effect

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.

- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.

Notes

- Only physical ports can be added to an AP port.
- The ports of different media types or port modes cannot be added to the same AP port.
- Layer-2 ports can be added to only a Layer-2 AP port, and Layer-3 ports can be added to only a Layer-3 AP port. The Layer-2/3 attributes of an AP port that contains member ports cannot be modified.
- After a port is added to an AP port, the attributes of the port are replaced by those of the AP port.
- After a port is removed from an AP port, the attributes of the port are restored.

After a port is added to an AP port, the attributes of the port are consistent with those of the AP port. Therefore, do not perform configuration on the AP member ports or apply configuration to a specific AP member port. However, some configurations (the **shutdown** and **no shutdown** commands) can be configured on AP member ports. When you use AP member ports, check whether the function that you want to configure can take effect on a specific AP member port, and perform this configuration properly.

The static aggregation has no error detection. Member ports are bound if linked up, so the user needs to ensure topology accuracy and consistency among member ports' negotiation attributes.

Configuration Steps

Creating an Ethernet AP Port

- Mandatory.
- Perform this configuration on an AP-enabled device.

Command	**interface aggregateport** *ap-number*
Parameter Description	*ap-number*: Indicates the number of an AP port.
Defaults	By default, no AP port is created.
Command Mode	Global configuration mode
Usage Guide	To create an Ethernet AP port, run **interface aggregateport** in global configuration mode. To delete the specified Ethernet AP port, run **no interface aggregateport** *ap-number* in global configuration mode.

Run **port-group** to add a physical port to a static AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.

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).

Configuring Static AP Member Ports

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

Command	**port-group** *ap-number*
Parameter Description	**port-group** *ap-number*: Indicates the number of an AP port.
Defaults	By default, no ports are added to any static AP port.
Command Mode	Interface configuration mode of the specified Ethernet port
Usage Guide	To add member ports to an AP port, run **port-group** in interface configuration mode. To remove member ports from an AP port, run **no port-group** in interface configuration mode.

- The static AP member ports configured on the devices at both ends of a link must be consistent.
- After a member port exits the AP port, the default settings of the member port are restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an AP port.
- After a member port exits an AP port, the port is disabled by using the **shutdown** command to avoid loops. After you confirm that the topology is normal, run **no shutdown** in interface configuration mode to enable the port again.

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 Description	*sub-ap-number*: Indicates the number of an AP subinterface.
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

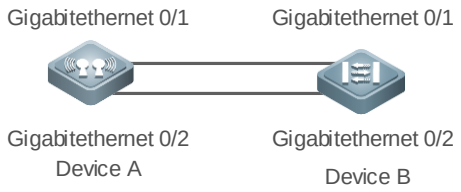
- Run **show running** to display the configuration.
- Run **show aggregateport summary** to display the AP configuration.

Command	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on all AP ports is displayed if you do not specify the AP port number.
	Hostname# show aggregateport 1 summary

	AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring an Ethernet Static AP Port

Scenario Figure 1-1	
Configuration Steps	● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP port 1. ● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP port 1.
DeviceA	DeviceA# configure terminal DeviceA(config)# interface range GigabitEthernet 0/1-2 DeviceA(config-if-range)# port-group 1
DeviceB	DeviceB# configure terminal DeviceB(config)# interface range GigabitEthernet 0/1-2 DeviceB(config-if-range)# port-group 1
Verification	● Run **show aggregateport summary** to check whether AP port 1 contains member ports GigabitEthernet 0/1 and GigabitEthernet 0/2.
DeviceA	DeviceA# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag1** 8 Enabled ACCESS **Gi0/1,Gi0/2**
DeviceB	DeviceB# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag1** 8 Enabled ACCESS **Gi2/1,Gi0/2**

1.4.2 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.

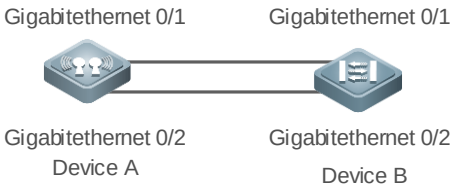
Command	**aggregateport member linktrap**
Parameter Description	N/A
Defaults	By default, LinkTrap is disabled for AP member ports.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to enable LinkTrap for all AP member ports. By default, LinkTrap messages 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 1-2	
Configuration Steps	• Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on DeviceA to static AP port 1. • Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on DeviceB to static AP port 1. • On DeviceA, disable LinkTrap for AP port 1 and enable LinkTrap for its member ports. • On DeviceB, disable LinkTrap for AP port 1 and enable LinkTrap its AP member ports.
DeviceA	DeviceA# configure terminal DeviceA(config)# interface range GigabitEthernet 0/1-2 DeviceA(config-if-range)# port-group 1 DeviceA(config-if-range)# exit DeviceA(config)# aggregateport member linktrap DeviceA(config)# interface Aggregateport 1 DeviceA(config-if-AggregatePort 1)# no snmp trap link-status
DeviceB	DeviceB# configure terminal DeviceB(config)# interface range GigabitEthernet 0/1-2 DeviceB(config-if-range)# port-group 1 DeviceB(config-if-range)# exit DeviceB(config)# aggregateport member linktrap DeviceB(config)# interface Aggregateport 1 DeviceB(config-if-AggregatePort 1)# no snmp trap link-status
Verification	• Run **show running** to check whether LinkTrap is enabled for AP port 1 and its member ports.
DeviceA	DeviceA# show run | include AggregatePort 1 Building configuration... Current configuration: 54 bytes

	interface AggregatePort 1 no snmp trap link-status DeviceA# show run | include AggregatePort aggregateport member linktrap
DeviceB	DeviceB# show run | include AggregatePort 1 Building configuration... Current configuration: 54 bytes interface AggregatePort 1 no snmp trap link-status DeviceB# show run | include AggregatePort aggregateport member linktrap

1.4.3 Configuring a Load Balancing Mode

Configuration Effect

The system distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links. A device enabled with enhanced load balancing first determines the type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

- In enhanced load balancing mode, configure the hash disturbance factor to ensure that same packets from two devices of the same type will be balanced to different links.
- In enhanced load balancing mode, enable hash synchronization to ensure that uplink and downlink packets of the same type will be transmitted over the same link. For example, in load balancing based on the source and destination IP addresses, enable hash synchronization for IPv4 packets to ensure that the uplink and downlink IPv4 packets will be transmitted over the same path.
- Enable flexible hash to balance traffic of a faulty link over an AP member port to other active links without affecting original data streams on these active links.

Notes

- Different disturbance factors may lead to the same disturbance effect.
- Enable or disable hash synchronization for IPv4, IPv6, FCoE and On as required.
- The flexible hash function can be configured in global configuration mode or interface configuration mode of a specific AP port.

Configuration Steps

↘ **Configuring the Global Load Balancing Algorithm of an AP port**

- (Optional) Perform this configuration when you need to optimize load balancing.
- Perform this configuration on AP-enabled devices.

Command	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip | src-dst-ip-l4port | enhanced profile** *profile-name* | **src- l4port** | **dst-l4port** | **src-dst-l4port** | **src-ip-src-l4port** | **src-ip-dst-l4port** | **dst-ip-src-l4port** | **dst-ip-dst-l4port** | **src-ip-src-dst-l4port** | **dst-ip-src-dst-l4port** | **src-dst-ip-src-l4port** | **src-dst-ip-dst-l4port | src-port | mpls-label | round-robin** }
Parameter Description	**dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming packets. **src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming packets. **src-dst-ip**: Indicates that load is distributed based on source and destination IP addresses of incoming packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming packets. **src-ip**: Indicates that load is distributed based on the source IP addresses of incoming packets. **src-dst-mac**: Indicates that load is distributed based on source and destination MAC addresses of incoming packets. **src-dst-ip-l4port**: Indicates that load is distributed based on source IP and destination IP addresses as well as Layer-4 source and destination port numbers. **enhanced profile** *profile-name*: Indicates the name of the enhanced load balancing profile. **src- l4port**: Indicates that load is distributed based on Layer-4 source port numbers. **dst- l4port**: Indicates that load is distributed based on Layer-4 destination port numbers. **src-dst-l4port**: Indicates that load is distributed based on Layer-4 source and destination port numbers. **src-ip-src-l4port**: Indicates that load is distributed based on source IP addresses and Layer-4 source port numbers. **src-ip-dst-l4port**: Indicates that load is distributed based on source IP addresses and Layer-4 destination port numbers. **dst-ip-src-l4port**: Indicates that load is distributed based on destination IP addresses and Layer-4 source port numbers. **dst-ip-dst-l4port**: Indicates that load is distributed based on destination IP addresses and Layer-4 destination port numbers. **src-ip-src-dst-l4port:** Indicates that load is distributed based on source IP addresses as well as Layer-4 source and destination port numbers. **dst-ip-src-dst-l4port**: Indicates that load is distributed based on destination IP addresses as well as Layer-4 source and destination port numbers. **src-dst-ip-src-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer-4 source port numbers. **src-dst-ip-dst-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer-4 destination port numbers. **src-port**: Indicates that load is distributed based on the panel port for incoming packets. **mpls-label**: Indicates that load is distributed based on the labels of MPLS packets. **round-robin**: Indicates that load is distributed by member port polling.

Defaults	Load balancing can be based on source and destination MAC addresses (applicable to switches), source and destination IP addresses (applicable to gateways), or the profile of enhanced load balancing (applicable to switches with CB line cards).
Command Mode	Global configuration mode
Usage Guide	To restore the default settings, run **no aggregateport load-balance** in global configuration mode. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run **no aggregateport load-balance** in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port.

Renaming the Profile of Enhanced Load Balancing

- By default, if a device supports enhanced load balancing, the system creates a profile named **default** for enhanced load balancing. Perform this configuration when you need to rename the profile or restore the default settings. In other cases, the configuration is optional.
- Perform this configuration on devices that support enhanced load balancing, such as aggregation switches and core switches.

Command	**load-balance-profile** *profile-name*
Parameter Description	*profile-name*: Indicates the profile name, which contains up to 31 characters.
Defaults	The default profile name is **default**.
Command Mode	Global configuration mode
Usage Guide	To enter default profile mode, run **load-balance-profile default**. To rename the enhanced load balancing profile, run **load-balance-profile** *profile-nam*. To restore the default profile name, run **default load-balance-profile** in global configuration mode. To restore the default load balancing settings, run **default load-balance-profile** *profile-name* in global configuration mode. Only one profile is supported globally. Please do not delete the profile. To display the enhanced load balancing profile, run **show load-balance-profile**.

Verification

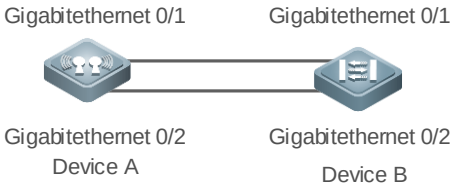
- Run **show running** to display the configuration.
- Run **show aggregateport load-balance** to display the load balancing configuration. If a device supports load balancing configuration on a specific AP port, run **show aggregateport summary** to display the configuration.
- Run **show load-balance-profile** to display the enhanced load balancing profile.

Command	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Parameter	*aggregate-port-number*: Indicates the number of an AP port.

Description	**load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on All AP ports is displayed if you do not specify the AP port number.
	Hostname# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring a Load Balancing Mode

Scenario Figure 1-3	
Configuration Steps	● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on DeviceA to static AP port 1. ● Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on DeviceB to static AP port 1. ● On DeviceA, configure source MAC address-based load balancing for AP port 1 in global configuration mode. ● On DeviceB, configure destination MAC address-based load balancing for AP port 1 in global configuration mode.
DeviceA	DeviceA# configure terminal DeviceA(config)# interface range GigabitEthernet 0/1-2 DeviceA(config-if-range)# port-group 1 DeviceA(config-if-range)# exit DeviceA(config)# aggregateport load-balance src-mac
DeviceB	DeviceB# configure terminal DeviceB(config)# interface range GigabitEthernet 0/1-2 DeviceB(config-if-range)# port-group 1 DeviceB(config-if-range)# exit DeviceB(config)# aggregateport load-balance dst-mac
Verification	● Run **show aggregateport load-balance** to check the load balancing algorithm

	configuration.
DeviceA	DeviceA# show aggregatePort load-balance Load-balance : **Source MAC**
DeviceB	DeviceB# show aggregatePort load-balance Load-balance : **Destination MAC**

Common Errors

A user enables hash synchronization for IPv4, IPv6, FCoE and On packets. However, no configuration is displayed when the user runs **show running**. This is because hash synchronization for IPv4, IPv6, and FCoE packets is enabled by default. After the user disables the function, the configuration is displayed.

1.5 Monitoring

Displaying

Description	Command
Displays the summary or load balancing algorithm of an AP port.	**show aggregateport** [*ap-number*] { **load-balance** | **summary** }

Debugging

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

Description	Command
Debugs an AP port.	**debug lsm ap**

Configuring Ethernet Switching

1. Configuring MAC Address
2. Configuring VLAN
3. Configuring LLDP

1 Configuring MAC Address

1.1 Overview

A MAC address table contains the MAC addresses, interface numbers and VLAN IDs of the devices connected to the local device.

When a device forwards a packet, it finds an output port from its MAC address table according to the destination MAC address and the VLAN ID of the packet.

After that, the packet is unicast, multicast or broadcast.

This document covers dynamic MAC addresses, static MAC addresses and filtered MAC addresses. For the management of multicast MAC addresses, please see *Configuring IGMP Snooping Configuration*.

Protocols and Standards

- IEEE 802.3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q: Virtual Bridged Local Area Networks

1.2 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 Through 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 Through 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.

Features

Feature	Description
Limiting on Dynamic MAC Addresses Learned in a VLAN	Limits the number of dynamic MAC addresses in a VLAN.
Limiting on Dynamic MAC Addresses Learned on an Interface	Limits the number of dynamic MAC addresses learned on an interface.

1.2.1 Limiting on Dynamic MAC Addresses Learned in a VLAN

Working Principle

The MAC address table with a limited capacity is shared by all VLANs on the device. If a large amount of MAC addresses in the MAC address table are learned in a VLAN, MAC addresses in other VLANs cannot be learned. As a result, packets in other VLANs are broadcast. To address this issue, the device provides limiting on dynamic MAC addresses learned in a VLAN. That is, you can configure the maximum number of dynamic MAC addresses learned in a VLAN.

With this function configured, the device can only learn a limited number of dynamic MAC addresses in a VLAN. The device does not learn MAC addresses of packets exceeding the limit. Instead, the device directly forwards such packets.

You can configure the device to drop packets exceeding the limit. When the maximum number of MAC addresses learned exceeds the limit, the device stops learning MAC address and discards the packets.

- If the number of learned MAC addresses is larger than the limit, the device stops learning MAC addresses in a VLAN. The device learns MAC addresses again only when the number of MAC addresses minus the number of aged MAC addresses in the VLAN falls below the limit.
- The MAC addresses copied to a specific VLAN are not subject to the limit.

1.2.2 Limiting on Dynamic MAC Addresses Learned on an Interface

Working Principle

An interface can only learn a limited number of dynamic MAC addresses after the limit is configured. The interface does not learn MAC addresses of packets exceeding the limit. Instead, the device interface directly forwards such packets.

You can configure the device to drop packets exceeding the limit. When the maximum number of MAC addresses learned exceeds the limit, the device stops learning MAC address and discards the packets.

- If the number of learned MAC addresses on an interface is larger than the limit, the device stops learning MAC addresses on the interface. The device learns MAC addresses again only when the number of MAC addresses minus the number of aged MAC addresses on the interface falls below the limit.

1.3 Configuration

Configuration	Description and Command	
Configuring Dynamic MAC Address	(Optional) It is used to configure the aging time of MAC addresses.	
	mac-address-table aging-time *seconds*	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 *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*	Configures a static MAC address.
Configuring a MAC Address for Packet Filtering	(Optional) It is used to filter packets.	
	ac-address-table filtering *mac-address* **vlan** *vlan-id*	Configures a MAC address for packet filtering.

1.3.1 Configuring Dynamic MAC Address

Configuration Effect

Learn MAC addresses dynamically and forward packets via unicast.

Notes

- N/A

Configuration Steps

Configuring an Aging Time for a Dynamic MAC Address

- Optional.
- Configure an aging time for dynamic MAC addresses.
-

Command	**mac-address-table aging-time** *value*
Parameter Description	*value*: indicates the aging time. The value is either 0 or in the range from 10 to 630.
Defaults	The default value is 300s.
Command Mode	Global configuration mode
Usage Guide	If the value is set to 0, MAC address aging is disabled and learned MAC addresses will not be aged.

The actual aging time may be different from the configured value, but it is not more than two times of the configured value.

Verification

- Check whether a device learns dynamic MAC addresses.
- Run the **show mac-address-table dynamic** command to display dynamic MAC addresses.
- Run the **show mac-address-table aging-time** command to display the aging time for dynamic MAC addresses.

Command	**show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: displays the information of a specific dynamic MAC address. **interface** *interface-type interface-number*: specifies a physical interface or an AP port. **vlan** *vlan-id*: displays the dynamic MAC addresses in a specific VLAN.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A

```
Hostname# show mac-address-table dynamic
Vlan        MAC Address          Type             Interface
----        ------------         ------           -------------------
1           0000.0000.0001       DYNAMIC    GigabitEthernet 0/1
1           0001.960c.a740       DYNAMIC    GigabitEthernet 0/1
1           0007.95c7.dff9       DYNAMIC    GigabitEthernet 0/1
1           0007.95cf.eee0       DYNAMIC    GigabitEthernet 0/1
1           0007.95cf.f41f       DYNAMIC    GigabitEthernet 0/1
1           0009.b715.d400       DYNAMIC    GigabitEthernet 0/1
1           0050.bade.63c4       DYNAMIC    GigabitEthernet 0/1
```

Field	Description
Vlan	Indicates the VLAN where the MAC address resides.
MAC Address	Indicates a MAC Address.
Type	Indicates a MAC address type.
Interface	Indicates the interface where the MAC address resides.

Command	**show mac-address-table aging-time**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A

```
Hostname# show mac-address-table aging-time
```

	Aging time: 300

Configuration Example

Configuring a Dynamic MAC Address

Scenario **Figure 1-1**	
Configuration Steps	● Configure the aging time for dynamic MAC addresses to 180s. ● Delete all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	Hostname# configure terminal Hostname(config)# mac aging-time 180 Hostname# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Verification	● Check MAC address learning on an interface. ● Check the aging time for dynamic MAC addresses. ● Check all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	Hostname# show mac-address-learning GigabitEthernet 0/1 learning ability: enable Hostname# show mac aging-time Aging time : 180 seconds Hostname# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1 Vlan MAC Address Type Interface ---------- ---------- -------- ---------- 1 00d0.f800.1001 STATIC GigabitEthernet 0/1

Common Errors

Configure MAC address learning on an interface before configuring the interface as a layer-2 interface, for example, a switch port or an AP port.

1.3.2 Configuring a Static MAC Address

Configuration Effect

- Bind the MAC address of a network device with a port of a switch.

Notes

- N/A

Configuration Steps

Configuring a Static MAC address

- Optional.
- Bind the MAC address of a network device with a port of a switch.

Command	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-type interface-number*
Parameter Description	**address** *mac-address*: specifies a MAC address. **vlan** *vlan-id*: specifies a VLAN where the MAC address resides. **interface** *interface-type interface-number*: specifies a physical interface or an AP port.
Defaults	By default, no static MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	When the switch receives a packet containing the specified MAC address on the specified VLAN, the packet is forwarded to the bound interface.

Verification

- Run the **show mac-address-table static** command to check whether the configuration takes effect.

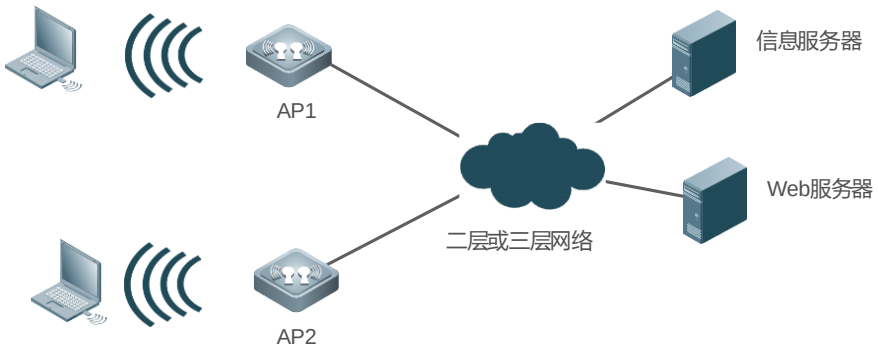
Command	**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: specifies a MAC address. **interface** *interface-type interface-number*: specifies a physical interface or an AP port. **vlan** *vlan-id*: specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
	Hostname# show mac-address-table static Vlan MAC Address Type Interface ----- ----------- -------- ------------------ 1 00d0.f800.1001 STATIC GigabitEthernet 0/1 1 00d0.f800.1002 STATIC GigabitEthernet 0/1 1 00d0.f800.1003 STATIC GigabitEthernet 0/1

Configuration Example

Configuring a Static MAC address

In the preceding example, the relationship of MAC addresses, VLAN IDs, and interface numbers is shown in the following table.

Role	MAC Address	VLAN ID	Interface Number
Web server	00d0.f800.3232	VLAN2	Gi0/1
Database server	00d0.f800.3233	VLAN2	Gi0/1

Scenario Figure 1-2	
Configuration Steps	● Specify destination MAC addresses (*mac-address*). ● Specify the VLAN (*vlan-id*) where the MAC addresses reside. ● Specify interface IDs (*interface-type interface-number*).
A	A# configure terminal A(config)# mac-address-table static 00d0.f800.3232 vlan 2 interface gigabitethernet 0/1 A(config)# mac-address-table static 00d0.f800.3233 vlan 2 interface gigabitethernet 0/1
Verification	Display the static MAC address configuration on a device.
A	A# show mac-address-table static Vlan MAC Address Type Interface ---------- ---------- ---------- ---------- 2 00d0.f800.3232 STATIC GigabitEthernet 0/1 2 00d0.f800.3233 STATIC GigabitEthernet 0/1 2 00d0.f800.3234 STATIC GigabitEthernet 0/1

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.

1.3.3 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.

Notes

- N/A

Configuration Steps

↘ **Configuring a MAC Address for Packet Filtering**

- Optional.
- Perform this configuration to filter packets.

Command	**mac-address-table filtering** *mac-address* **vlan** *vlan-id*
Parameter Description	**address** *mac-address*: specifies a MAC address. **vlan** *vlan-id*: specifies a VLAN where the MAC address resides.
Defaults	By default, no filtered MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Verification

- Run the **show mac-address-table filter** command to display the filtered MAC address.

Command	**show mac-address-table filter** [**address** *mac-address*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: specifies a MAC address. **vlan** *vlan-id*: specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	Hostname# show mac-address-table filtering Vlan MAC Address Type Interface ------ ---------- -------- ---------- 1 0000.2222.2222 FILTER

Configuration Example

Configuring a MAC Address for Packet Filtering

Configuration Steps	• Specify a destination MAC address (*mac-address*) for filtering. • Specify a VLAN where the MAC addresses resides.
	Hostname# configure terminal Hostname(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1
Verification	Display the filtered MAC address configuration.
	Hostname# show mac-address-table filter Vlan MAC Address Type Interface ---------- ---------- -------- ---------- 1 00d0.f800.3232.0001 FILTER

Common Errors

N/A

1.4 Monitoring

Clearing

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

Description	Command
Clears dynamic MAC addresses.	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]

Displaying

Description	Command
Displays the MAC address table.	**show mac-address-table** { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]
Displays the aging time for dynamic MAC addresses.	**show mac-address-table aging-time**
Displays the number of address entries in the address table.	**show mac-address-table count** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]
Displays all the MAC addresses on the specified interface including static and dynamic MAC addresses.	**show mac-address-table interface** [*interface-type interface-number*] [**vlan** *vlan-id*]
Displays the MAC address learning.	**show mac-address-learning**
Displays all addresses of the specified VLAN.	**show mac-address-table vlan** [*vlan-id*]

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**

1 Configuring VLAN

1.1 Overview

A virtual local area network (VLAN) is a logical network created on a physical network. Each VLAN has an independent broadcast domain, and different VLANs are isolated at Layer 2. Devices in different VLANs can interwork with each other through Layer 3 devices or interfaces.

Protocols and Standards

- IEEE 802.1Q Virtual Bridged Local Area Networks and Standards

1.2 Features

Basic Concepts

VLAN

A VLAN is a logical network created based on a physical network. A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

- The VLANs supported by 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.
- The configurable VLAN IDs are from 1 to 4094.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.

Interface Types

You can configure an interface type to determine the frames allowed to pass through an interface and the VLANs which the interface belongs to. The following table lists interface types.

Interface Type	Description
Access interface	An access interface belongs to only one VLAN and is specified manually.
Trunk interface (IEEE 802.1Q)	A trunk interface belongs to all the VLANs of the device by default and can forward frames of all the VLANs. You can configure allowed VLANs for the trunk interface.
Uplink interface	An uplink interface belongs to all the VLANs of the device by default and can forward frames of all the VLANs. It forwards frames of the native VLAN in tagged mode.
Hybrid interface	A hybrid interface belongs to all the VLANs of the device by default and can forward frames of all the VLANs. It can forward frames of multiple VLANs in untagged mode. You can configure allowed VLANs for the hybrid interface.

Features

Feature	Description
VLAN	Implements Layer 2 isolation.

1.1.1 VLAN

Each VLAN has an independent broadcast domain, and different VLANs are isolated at Layer 2.

Working Principle

Each VLAN has an independent broadcast domain, and different VLANs are isolated at Layer 2.

1.3 Configuration

Configuration	Description and Command	
Configuring VLAN	(Mandatory) It is used to create a VLAN.	
	vlan { *vlan-id* | **range** *vlan-range* }	Enters a VLAN ID.
	(Optional) It is used to rename a VLAN.	
	name *vlan-name*	Names a VLAN.
	Optional.	
	interface vlan	Creates a Layer 3 SVI of a VLAN.
Configuring VLAN Encapsulation for an Interface	(Mandatory) It is used to configure VLAN encapsulation for an interface.	
	encapsulation	Configures VLAN encapsulation for an interface or sub-interface.

1.3.1 Configuring VLAN

Configuration Effect

- A VLAN is identified by a VLAN ID. You may add, delete, or modify VLANs 2 to 4094, but VLAN 1 is created automatically and cannot be deleted.

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 the VLAN mode.

Command	**vlan** { *vlan-id* | **range** *vlan-range* }
Parameter Description	*vlan-id*: indicates the VLAN ID ranging from 1 to 4094. **range** *vlan-range*: indicates the VLAN ID range.
Defaults	VLAN 1 is created automatically and cannot be deleted.
Command Mode	Global configuration mode
Usage Guide	If you enter a new VLAN ID, the corresponding VLAN will be created. If you enter an existing VLAN ID, the corresponding VLAN will be modified. You may use the **no vlan** *vlan-id* command to delete a VLAN. The undeletable VLANs include VLAN1.

Renaming a VLAN

- Optional.
- You cannot rename a VLAN the same as the default name of another VLAN.

Command	**name** *vlan-name*
Parameter Description	*vlan-name*: Indicates a VLAN name.
Defaults	By default, the name of a VLAN is its VLAN ID. For example, the default name of the VLAN 4 is VLAN 0004.
Command Mode	VLAN configuration mode
Usage Guide	To restore the VLAN name to defaults, use the **no name** command.

Configuring a BVI

- Optional.
- Create a Layer 3 bridge virtual interface (BVI) for a VLAN, enter the BVI configuration mode, and assign an IP address to the BVI so that devices in the VLAN can communicate at Layer 3.

Command	**interface bvi** *bvi-id*
Parameter Description	*bvi-id*: indicates the VLAN ID.
Defaults	No BVI exists in a VLAN by default.
Command Mode	Global configuration mode, VLAN configuration mode, or interface configuration mode
Usage Guide	-

Verification

- Run the **show vlan** [**id** *vlan-id*] command to check whether the VLAN configuration takes effect.
- Run the **show interface bvi** bvi-id command to check detailed BVI configuration.

Configuration Examples

Configuring a VLAN

Configuration Steps

- Create a VLAN and rename it **test888**.

```
Hostname# configure terminal
Hostname(config)# vlan 888
Hostname(config-vlan)# name test888
```

Verification Run the **show** vlan [**id** *vlan-id*] command to check whether the VLAN configuration is correct.

```
Hostname(config-vlan)#show vlan
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -----------------------------------
   1 VLAN0001                            STATIC
888 test888                              STATIC
```

↘ Configuring an BVI

Configuration Steps Create an SVI for VLAN 1 and assign an IP address to the BVI.

```
Hostname# configure terminal
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip address 10.10.29.1/24
Hostname(config-if-BVI 1)# end
```

Verification Run the **show interface bvi** *bvi-id* command to check detailed BVI configuration.

```
Index(dec):5 (hex):5
BVI 1 is UP    , line protocol is UP
  Hardware is BVI, address is 00d0.f822.33f3 (bia 00d0.f822.33f3)
  Interface address is: 172.29.25.201/24
  ARP type: ARPA, ARP Timeout: 3600 seconds
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

1.3.2 Configuring VLAN Encapsulation for an Interface

Configuration Effect

- Configure VLAN encapsulation for an interface or sub-interface.

Configuration Steps

↘ Configure VLAN encapsulation for an interface or sub-interface.

- Mandatory.

Command	**encapsulation dot1q** *vlan-id*
Parameter Description	*vlan-id*: Specifies the VLAN ID. The value ranges from 1 to 4094.

Defaults	An interface or sub-interface does not encapsulate any VLAN ID into packets by default.
Command Mode	Interface configuration mode
Usage Guide	When VLAN encapsulation is configured for an interface, the interface type is hybrid. The VLAN IDs to be encapsulated into packets on an interface or all its sub-interfaces must be unique. You can run the **no encapsulation** command to configure an interface or sub-interface not to encapsulate any VLAN ID into packets. You can use the default form of the command to restore default settings of an interface or sub-interface.

Verification

- You can run the **show interface** command to check the VLAN ID to be encapsulated into packets on an interface or sub-interface. You can run the **show vlan** command to check the interfaces added to VLANs.

Configuration Examples

↘ Configuring VLAN Encapsulation for an Interface or Sub-interface

Configuration Steps Add GigabitEthernet 0/1 to VLAN 1 and GigabitEthernet 0/1.1 to VLAN 2.

```
Hostname> enable
Hostname(config)# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# encapsulation dot1q 1
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# interface gigabitethernet 0/1.1
Hostname(config-subif-GigabitEthernet 0/1.1)# encapsulation dot1q 2
Hostname(config-subif-GigabitEthernet 0/1.1)# exit
```

Verification Run the **show interface** command to check the VLAN ID to be encapsulated into packets on GigabitEthernet 0/1.

```
Index(dec):2 (hex):2
GigabitEthernet 0/2 is DOWN , line protocol is DOWN
  Hardware is BCM47622 GigabitEthernet, address is 00d0.f019.911b (bia 00d0.f019.911b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 1970-01-01 08:00:35
```

```
    Time duration since last link state change: 5 days,    4 hours, 13 minutes, 43 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
  Bridge attributes:
    Port-type: hybrid
    Tagged vlan id: none
    Untagged 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 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 no buffer, 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

Run the **show interface** command to check the VLAN ID to be encapsulated into packets on GigabitEthernet 0/1.1.

```
ifindex(dec):8 (hex):8
GigabitEthernet 0/2.1 is DOWN    , line protocol is DOWN
  Hardware is BCM47622 GigabitEthernet, address is 00d0.f019.911b (bia 00d0.f019.911b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is 802.1Q Virtual LAN,Vlan ID 2
```

Run the **show vlan** command to check the interfaces added to VLANs.

```
Hostname#show vlan
VLAN           Name                                  Status       Ports
---------- -------------------------------- --------- -----------------------------------
             1 VLAN0001                              STATIC       Gi0/1
             2 VLAN0002                              STATIC       Gi0/1.1
```

1.4 Monitoring

Displaying

Description	Command
Displays VLAN configuration.	**show vlan** [**id** *vlan-id*]
Displays configurations of switch ports.	**show interface** [*interface-type interface-number*] **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**

1 Configuring LLDP

1.1 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 the topology, for example, device ports connected to other devices and check whether the rates and duplex modes at both ends of a link are consistent. An administrator can quickly locate and rectify a fault based on the information.

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

- LLDP-compliant device
- Endpoint device that complies with the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)

Protocols and Standards

- IEEE 802.1AB 2005: Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

1.2 Applications

Application	Description
Displaying Topology	Multiple switching devices, a MED device, and an NMS are deployed in the network topology.
Conducting Error Detection	Two switching devices are directly connected and incorrect configuration will be displayed.

1.2.1 Displaying Topology

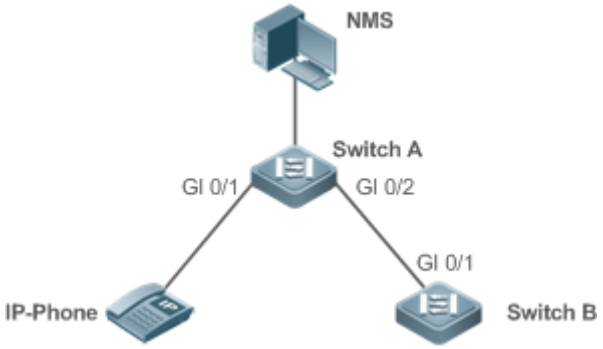
Scenario

Multiple switching devices, a MED device, and an NMS are deployed in the network topology.

As shown in the following figure, LLDP 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 (IP phone) through GigabitEthernet 0/1.
- The NMS accesses MIB of Switch A.

Figure 1-1



Remarks	Switch A, Switch B, and the IP phone support LLDP and LLDP-MED. LLDP on switch device 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 device 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.

1.2.2 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), the port rate and duplex mode, link aggregation, and maximum transmission unit (MTU) of the port on Switch A, an error will be prompted if the configuration does not match that on Switch B, and vice versa.

Figure 1-2



Remarks	Switch A and Switch B support LLDP. LLDP on switch device 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 device to implement neighbor discovery and detect link fault.

1.3 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 1-3 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

LLDPDUs can be encapsulated in two formats: Ethernet II and Subnetwork Access Protocols (SNAP).

The following figure shows the format of LLDPDUs encapsulated in the Ethernet II format.

Figure 1-4 Ethernet II Format

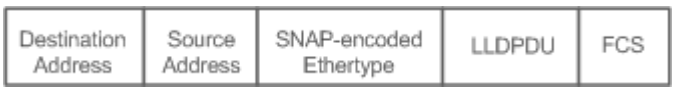


In the preceding figure:

- 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 data unit.
- FCS: indicates the frame check sequence.

Figure 1-5 shows the format of LLDPDUs encapsulated in SNAP format.

Figure 1-5 SNAP Format



In the preceding figure:

- Destination Address: indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.
- Source Address: indicates the source MAC address, which is the port MAC address.

- SNAP-encoded Ethertype: indicates the Ethernet type of the SNMP encapsulation, which is AA-AA-03-00-00-00-88-CC.
- LLDPDU: indicates the LLDP protocol data unit.
- FCS: indicates the frame check sequence.

TLV

TLVs encapsulated into an LLDPDU can be classified into two types: Basic management TLVs and organizationally specific TLVs

Basic management TLVs are a collection of basic TLVs used for network management. Organizationally specific TLVs are defined by standard organizations and other institutions, for example, the IEEE 802.1 organization and IEEE 802.3 organization define their own TLV collections.

1. Basic management TLVs

The basic management TLV collection consists of two types of TLVs: mandatory TLVs and optional TLVs. A mandatory TLV must be contained in an LLDPDU for advertisement and an optional TLV is contained selectively.

TLV Type	Description	Mandatory/Optional
End Of LLDPDU TLV	Indicates the end of an LLDPDU, occupying two bytes.	Mandatory
Chassis ID TLV	Identifies a device with a MAC address.	Mandatory
Port ID TLV	Identifies a port sending LLDPDUs.	Fixed
Time To Live TLV	Indicates the time to live (TTL) of local information on a neighbor. When a device receives a TLV containing TTL 0, it deletes the neighbor information.	Mandatory
Port Description TLV	Indicates the descriptor of the port sending LLDPDUs.	Optional
System Name TLV	Describes the device name.	Optional
System Description TLV	Indicates the device description, including the hardware version, software version, and operating system information.	Optional
System Capabilities TLV	Describes main functions of the device, such as the bridge, routing, and relay functions.	Optional
Management Address TLV	Indicates the management address, which contains the interface ID and object identifier (OID).	Optional

LLDP-compliant switches support advertisement of basic management TLVs.

2. Organizationally specific TLVs

Different organizations, such as the IEEE 802.1, IEEE 802.3, IETF and device suppliers, define specific TLVs to advertise specific information about devices. The organizationally unique identifier (OUI) field in a TLV is used to distinguish different organizations.

Organizationally specific TLVs are optional and are advertised in an LLDPDU selectively. Currently, there are three types of common organizationally specific TLVs: IEEE 802.1 organizationally specific TLVs, IEEE 802.3 organizationally specific TLVs, and IEEE 802.1AB LLDP-MED TLVs.

- IEEE 802.1 organizationally specific TLVs

The following table describes IEEE 802.1 organizationally specific TLVs.

TLV Type	Description
Port VLAN ID TLV	Indicates the VLAN identifier of a port.
Port And Protocol VLAN ID TLV	Indicates the protocol VLAN identifier of a port.
VLAN Name TLV	Indicates the VLAN name of a port.
Protocol Identity TLV	Indicates the protocol type supported by a port.

LLDP-compliant switches do not send the Protocol Identity TLV but receive this TLV.

- IEEE 802.3 organizationally specific TLVs

TLV Type	Description
MAC/PHY Configuration//Status TLV	Indicates the rate and duplex mode of a port, and whether to support and enable auto-negotiation.
Power Via MDI TLV	Indicates the power supply capacity of a port.
Link Aggregation TLV	Indicates the link aggregation capacity of a port and the current aggregation state.
Maximum Frame Size TLV	Indicates the maximum size of the frame transmitted by a port.

LLDP-compliant devices support advertisement of IEEE 802.3 organizationally specific TLVs.

- LLDP-MED TLV

LLDP-MED is an extension to LLDP based on IEEE 802.1AB LLDP. It enables users to conveniently deploy the Voice Over IP (VoIP) network and detect faults. It provides applications including the network configuration policies, device discovery, PoE management, and inventory management, meeting requirements for low cost, effective management, and easy deployment.

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.

LLDP-compliant Ruijie devices support advertisement of LLDP-MED TLVs.

Overview

Feature	Description
LLDP Working Mode	Configures the mode of transmitting and receiving LLDPDUs.
LLDP Transmission Mechanism	Enables directly connected LLDP-compliant devices to send LLDPDUs to the peer.
LLDP Reception Mechanism	Enables directly connected LLDP-compliant devices to receive LLDPDUs from the peer.

1.3.1 LLDP Working Mode

Configure the LLDP working mode so as to specify the LLDP packet transmission and reception mode.

Working Principle

LLDP provides three working modes:

- TxRx: LLDPDUs are received and transmitted.
- Rx Only: LLDPDUs are received only.
- Tx Only: LLDPDUs are transmitted only.

When the LLDP working 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 working mode.

Related Configuration

↘ Configuring the LLDP Working Mode

The default LLDP working mode is TxRx.

You can run the **lldp mode** command to configure the LLDP working mode.

If the working mode is set to TxRx, the device can both transmit and receive LLDPDUs. If the working mode is set to Rx Only, the device can only receive LLDPDUs. If the working mode is set to Tx Only, the device can only transmit LLDPDUs. If the working mode is disabled, the device cannot transmit or receive LLDPDUs.

1.3.2 LLDP Transmission Mechanism

LLDPDUs inform peers of their neighbors. When the LLDP transmission mode is cancelled or disabled, LLDPDUs cannot be transmitted to neighbors.

Working Principle

LLDP periodically transmits LLDPDUs when working in TxRx or Tx Only mode. When information about the local device changes, LLDP immediately transmits LLDPDUs. You can configure a delay time to avoid frequent transmission of LLDPDUs 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 working 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 working 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 LLDPDUs at an interval of 1 second.

Related Configuration

Configuring the LLDP Working Mode

The default working 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 LLDPDU reception, set the working mode to TxRx or Rx Only. If the working mode is set to Rx Only, the device can only receive LLDPDUs.

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 a small delay is used, the frequent change of local information will cause frequent transmission of LLDPDUs. If a large delay is used, LLDPDUs cannot be sent immediately upon local information change.

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, LLDPDUs 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 LLDPDUs are fast transmitted.

Run the **lldp fast-count** command to change the number of LLDPDUs that are fast transmitted.

1.3.3 LLDP Reception Mechanism

A device can discover the neighbor and determine whether to age the neighbor information according to received LLDPDUs.

Working Principle

A device can receive LLDPDUs 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 Working Mode

The default LLDP working mode is TxRx.

Run the **lldp mode txrx** or **lldp mode rx** command to enable the LLDPDU receiving function. Run the **lldp mode tx** or **no lldp mode** command to disable the LLDPDU receiving function.

In order to enable LLDPDU receiving, set the working mode to TxRx or Rx Only. If the working mode is set to Tx Only, the device can only transmit LLDPDUs.

1.4 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 Working Mode	⚠ (Optional) It is used to configure the LLDP working mode.	
	lldp mode { **rx** | **tx** | **txrx** }	Configures the LLDP working mode.
	no lldp mode	Restores the default LLDP working mode.
Configuring the TLVs to Be Advertised	⚠ (Optional) It is used to configure the TLVs to be advertised.	
	lldp tlv-enable basic-tlv	Configures an interface to advertise optional basic management TLVs.
	no lldp tlv-enable basic-tlv	Configures an interface not to advertise optional basic management TLVs.

Configuration	Description and Command	
	lldp tlv-enable dot1-tlv	Configures the IEEE 802.1 organizationally specific TLVs to be advertised.
	no lldp tlv-enable dot1-tlv	Cancels IEEE 802.1 organizationally specific TLVs.
	lldp tlv-enable dot3-tlv	Configures the IEEE 802.3 organizationally specific TLVs to be advertised.
	no lldp tlv-enable dot3-tlv	Cancels IEEE 802.3 organizationally specific TLVs.
	lldp tlv-enable med-tlv	Configures the LLDP-MED TLVs to be advertised.
	no lldp tlv-enable med-tlv	Cancels LLDP-MED TLVs.
Configures the Management Address to Be Advertised	⚠ (Optional) It is used to configure the management address to be advertised in LLDPDUs.	
	lldp management-address-tlv *ip-address*	Configures the management address to be advertised in LLDPDUs.
	no lldp management-address-tlv [*ip-address*]	Restores the default management address to be advertised in LLDPDUs.
Configuring the LLDP Fast Transmission Count	⚠ (Optional) It is used to configure the number of LLDPDUs that are fast transmitted.	
	lldp fast-count *fast-count-value*	Configures the LLDP fast transmission 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 *ttl-value*	Configures the TTL multiplier.
	no lldp hold-multiplier	Restores the default TTL multiplier.
	lldp timer tx-interval *tx-interval*	Configures the transmission interval.
	no lldp timer tx-interval	Restores the default LLDPDU transmission interval.
Configuring the Transmission Delay	⚠ (Optional) It is used to configure the delay for LLDPDU transmission.	
	lldp timer tx-delay *tx-delay*	Configures the transmission delay.
	no lldp timer tx-delay	Restores the default LLDPDU 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 *reinit-delay*	Configures the initialization delay.

Configuration	Description and Command	
	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 *trap*	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 *profile-num*	Configures an LLDP network policy.
	no lldp network-policy profile *profile-num*	Deletes an LLDP network policy.
	⚠ (Optional) It is used to configure a voice VLAN policy.	
	{ **voice** | **voice-signaling** } **vlan**	Configures a voice VLAN policy.
	no { **voice** | **voice-signaling** } **vlan**	Deletes a voice VLAN policy.
	⚠ (Optional) It is used to configure an interface to advertise an LLDP network policy.	
	lldp tlv-enable med-tlv network-policy profile [*profile-number*]	Configures an interface to advertise a network policy TLV.
	no lldp tlv-enable med-tlv network-policy profile [*profile-number*]	Configures an interface not to advertise a network policy TLV.
Configuring the Civic Address	⚠ (Optional) It is used to configure the LLDP civic address.	
	lldp location civic-location identifier *id*	Creates a civic address of a device.

Configuration	Description and Command	
	no lldp location civic-location identifier *id*	Deletes a civic address of a device.
	⚠ (Optional) It is used to configure the civic address of a device.	
	{ **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*	Configures the civic address of a device.
	no { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*	Deletes the civic address of a device.
	⚠ (Optional) It is used to configure the device type.	
	device-type *device-type*	Configures the device type.
	no device-type	Deletes the device type.
	⚠ (Optional) It is used to configure the TLVs to be advertised.	
	lldp tlv-enable med-tlv location civic-location identifier *id*	Configures the civic address in Location Identification TLV to be advertised.
	no lldp tlv-enable med-tlv location civic-location identifier *id*	Cancels the civic address in Location Identification TLV to be advertised.
Configuring the Emergency Telephone Number	⚠ (Optional) It is used to configure the emergency telephone number of a device.	
	lldp location elin identifier *id* **elin-location** *tel-number*	Configures the emergency telephone number of a device.
	no lldp location elin identifier *id*	Restores the default emergency telephone number on the device.
	⚠ (Optional) It is used to configure the TLVs to be advertised.	

Configuration	Description and Command	
	lldp tlv-enable med-tlv location elin identifier *id*	Configures the emergency telephone number in Location Identification TLV to be advertised.
	no lldp tlv-enable med-tlv location elin identifier *id*	Cancels the emergency telephone number in Location Identification TLV to be advertised.
Configuring the Function of Ignoring PVID Detection	⚠ (Optional) It is used to ignore PVID detection.	
	lldp ignore pvid-error-detect	Enables the function of ignoring PVID detection.
	no lldp ignore pvid-error-detect	Disables the function of ignoring PVID detection.

1.4.1 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.

↘ Enabling the LLDP Function

Command	**lldp enable**
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Global or 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.

Verification

Display the 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

Disabling the LLDP Function

Command	no lldp enable
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Global or interface configuration mode
Usage Guide	N/A

Configuration Example

Disabling the LLDP Function

Configuration Steps	Disable the LLDP function in global configuration mode.
	Hostname(config)#no lldp enable
Verification	Display global LLDP status.
	Hostname(config)#show lldp status Global status of LLDP: Disable

Common Errors

- If the LLDP function is enabled on an interface but disabled in global configuration mode, the LLDP function does not take effect on the interface.
- A port can learn a maximum of five neighbors.
- If a neighbor does not support LLDP but it is connected to an LLDP-supported device, a port may learn information about the device that is not directly connected to the port because the neighbor may forward LLDPDUs.

1.4.2 Configuring the LLDP Working Mode

Configuration Effect

- If you set the LLDP working mode to TxRx, the interface can transmit and receive packets.
- If you set the LLDP working mode to Tx, the interface can only transmit packets but cannot receive packets.
- If you set the LLDP working mode to Rx, the interface can only receive packets but cannot transmit packets.
- If you disable the LLDP working 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 working mode to Tx or Rx as required.

Configuring the LLDP Working Mode

Command	**lldp mode** { **rx** | **tx** | **txrx** }
Parameter Description	**rx**: Only receives LLDPDUs. **tx**: Only transmits LLDPDUs. **txrx**: Transmits and receives LLDPDUs.
Defaults	The default working mode is **txrx**, that is, LLDPDUs are received and transmitted.
Command Mode	Interface configuration mode
Usage Guide	To make LLDP take effect on an interface, enable LLDP globally and set the LLDP working mode on the interface to Tx, Rx, or TxRx.

Verification

Check the LLDP status on an interface.

Check whether the LLDP working mode on an interface is consistent with the configured one.

Related Commands

Disabling the LLDP Working Mode

Command	**no lldp mode**
Parameter Description	N/A
Defaults	The default working mode is **txrx**, that is, LLDPDUs are received and transmitted.
Command Mode	Interface configuration mode
Usage Guide	After the LLDP working mode on an interface is disabled, the interface does not transmit or receive LLDPDUs.

Configuration Example

Configuring the LLDP Working Mode

Configuration Steps	Set the LLDP working mode to **tx** in interface configuration mode.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp mode tx

Verification	Display LLDP status information on the interface.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : TxOnly Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

1.4.3 Configuring the TLVs to Be Advertised

Configuration Effect

- Configure the type of TLVs to be advertised to specify the LLDPDUs in LLDPDUs.

Notes

- When you specify **all** for basic management TLVs, IEEE 802.1 organizationally specific TLVs, and IEEE 802.3 organizationally specific TLVs, all optional TLVs of these types are advertised.
- When you specify **all** for LLDP-MED TLVs, all LLDP-MED TLVs except the Location Identification TLV are advertised.
- To configure the device to advertise the LLDP-MED Capability TLV, first configure the LLDP 802.3 MAC/PHY TLV. To cancel advertisement of the LLDP 802.3 MAC/PHY TLV, first cancel advertisement of the LLDP-MED Capability TLV.
- To configure LLDP-MED TLVs, configure the LLDP-MED Capability TLV before configuring other types of LLDP-MED TLVs. To cancel advertisement of the LLDP-MED Capability TLV, first cancel advertisement of other LLDP-MED TLVs. If the device connects to the IP phone that supports LLDP-MED, configure the network policy TLV so that policies can be delivered to the IP phone.

Configuration Steps

- Optional.
- Configure the type of TLVs to be advertised on an interface.

↘ **Configuring an Interface to Advertise Optional Basic Management TLVs**

Command	**lldp tlv-enable basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }

Parameter Description	**all**: indicates the Port Description TLV, System Capabilities TLV, System Description TLV, and System Name TLV of basic management TLVs. **port-description**: indicates the Port Description TLV, which describes an interface where LLDPDUs are received and transmitted. **system-capability**: indicates the System Capabilities TLV, which describes main functions supported by the device, such as bridging, routing, and relay functions. **system-description**: indicates the System Description TLV, which describes the hardware version, software version, operating system, and other information. **system-name**: indicates the System Name TLV, which describes the device name.
Defaults	By default, an interface advertises the Port Description TLV, System Capabilities TLV, System Description TLV, and System Name TLV.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring an Interface to Advertise 802.1 TLVs

Command	**lldp tlv-enable dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] }
Parameter Description	**all**: indicates the Port VLAN ID TLV, Port and Protocol VLAN ID TLV, and VLAN Name TLV of 802.1 TLVs. **port-vlan-id**: indicates the Port VLAN ID TLV, that is, VLAN ID of an interface. **protocol-vlan-id** [*vlan-id*]: indicates the Port and Protocol VLAN ID TLV, that is, interface and protocol VLAN ID. *vlan-id* indicates the VLAN ID. The value ranges from 1 to 4094. **vlan-name** [*vlan-id*]: indicates the VLAN Name TLV, that is, VLAN name of an interface. *vlan-id* indicates the VLAN ID. The value ranges from 1 to 4094.
Defaults	By default, an interface advertises the Port VLAN ID TLV, Port and Protocol VLAN ID TLV, and VLAN Name TLV.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring an Interface to Advertise 802.3 TLVs

Command	**lldp tlv-enable dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }
Parameter Description	**all**: indicates all optional TLVs of 802.3 TLVs. **link-aggregation**: indicates the Link Aggregation TLV, which describes the link aggregation capability of an interface and link aggregation status. **mac-physic**: indicates the MAC/PHY Configuration/Status TLV, which describes the rate and duplex mode of an interface, and whether auto-negotiation is supported and enabled. **max-frame-size**: indicates the Maximum Frame Size TLV, which describes the maximum frame size that can be transmitted by the interface. **power**: indicates the Power Via MDI TLV, which describes the power supply capability of an interface.
Defaults	By default, an interface advertises all 802.3 TLVs.

Command Mode	Interface configuration mode
Usage Guide	-

Configuring an Interface to Advertise LLDP-MED TLVs

Command	**lldp tlv-enable med-tlv** { **all** | **capability** | **inventory** | **location civic-location identifier** *id* | **location elin identifier** *id* | **network-policy profile** [*profile-number*] | **power-over-ethernet** }
Parameter Description	**all**: indicates that the device advertises LLDP-MED TLVs except the Location Identification TLV. **capability**: indicates the LLDP-MED Capabilities TLV, that is, whether the device supports LLDP-MED, types of LLDP-MED TLVs encapsulated into LLDPDUs, and device type (network device or endpoint device). **inventory**: indicates the inventory management TLV, that is, **media device** inventory management information. It contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location civic-location identifier** *id*: indicates the civic address information in the Location Identification TLV, including the common address and device type. **identifier** *id* specifies the civic address policy ID. The value ranges from 1 to 1024. You must first configure the LLDP civic address, and then configure the device to allow the TLV to be advertised. **location elin identifier** *id*: indicates the emergency telephone number to be encapsulated in the Location Identification TLV. **identifier** *id*: indicates the emergency telephone number configured in a policy of a specified ID. The value ranges from 1 to 1024. You must first configure the emergency telephone number, and then configure the device to allow the TLV to be advertised. **network-policy profile** [*profile-number*]: indicates the network policy TLV, notifying the VLAN configuration of the interface, supported application types (such as voice or video), Layer 2 or Layer 3 priority information, and other items. *profile-number* specifies the network policy ID. The value ranges from 1 to 1024. If the device is connected to the downstream IP phone that supports LLDP-MED, you can configure the network policy TLV on the device to deliver policies to the IP phone. You must first configure the network policy TLV, and then configure the device to allow the TLV to be advertised. **power-over-ethernet**: indicates the Extended Power-via-MDI TLV, that is, extended power supply capability.
Defaults	By default, an interface advertises all LLDP-MED TLVs except the Location Identification TLV.
Command Mode	Interface configuration mode
Usage Guide	-

Verification

Display the configuration of TLVs to be advertised on an interface

- Check whether the configuration takes effect.

Related Commands

Configuring an Interface Not to Advertise Optional Basic Management TLVs

Command	**no lldp tlv-enable basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }
Parameter Description	**all**: indicates the Port Description TLV, System Capabilities TLV, System Description TLV, and System Name TLV of basic management TLVs. **port-description**: indicates the Port Description TLV, which describes an interface where LLDPDUs are received and transmitted. **system-capability**: indicates the System Capabilities TLV, which describes main functions supported by the device, such as bridging, routing, and relay functions. **system-description**: indicates the System Description TLV, which describes the device hardware version, software version, operating system, and other information. "**system-name**" indicates the System Name TLV, which describes the device name.
Defaults	By default, an interface advertises the Port Description TLV, System Capabilities TLV, System Description TLV, and System Name TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring an Interface Not to Advertise 802.1 TLVs

Command	**no lldp tlv-enable dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** }
Parameter Description	**all**: indicates the Port VLAN ID TLV, Port and Protocol VLAN ID TLV, and VLAN Name TLV of 802.1 TLVs. **port-vlan-id**: indicates the Port VLAN ID, that is, VLAN ID of an interface. **protocol-vlan-id**: indicates the Port and Protocol VLAN ID TLV, that is, interface and protocol VLAN ID. *vlan-id* indicates the VLAN ID. The value ranges from 1 to 4094. **vlan-name**: indicates the VLAN Name TLV, that is, VLAN name of an interface. *vlan-id* indicates the VLAN ID. The value ranges from 1 to 4094.
Defaults	By default, an interface advertises the Port VLAN ID TLV, Port and Protocol VLAN ID TLV, and VLAN Name TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring an Interface Not to Advertise 802.3 TLVs

Command	**no lldp tlv-enable dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }
Parameter Description	**all**: indicates all the IEEE 802.3 organizationally specific TLVs are not advertised. **link-aggregation**: indicates the Link Aggregation TLV, which describes the link aggregation capability of an interface and link aggregation status. **mac-physic**: indicates the MAC/PHY Configuration/Status TLV, which describes the rate and duplex mode of an interface, and whether auto-negotiation is supported and enabled. **max-frame-size**: indicates the Maximum Frame Size TLV, which describes the maximum frame size that can be transmitted by the interface. **power**: indicates the Power Via MDI TLV, which describes the power supply capability of an interface.
Defaults	By default, an interface advertises all 802.3 TLVs.

Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring an Interface Not to Advertise LLDP-MED TLVs

Command	**no lldp tlv-enable med-tlv** { **all** | **capability** | **inventory** | **location civic-location identifier** *id* | **location elin identifier** *id* | **network-policy profile** [*profile-num*] | **power-over-ethernet** } }
Parameter Description	**all**: indicates that the device does not advertise LLDP-MED TLVs including the Location Identification TLV. **capability**: indicates the LLDP-MED Capabilities TLV, that is, whether the device supports LLDP-MED, types of LLDP-MED TLVs encapsulated into LLDPDUs, and device type (network device or endpoint device). **Inventory**: indicates the inventory management TLV, that is, media device inventory management information. It contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **Location civic-location identifier** *id*: indicates the civic address information in the Location Identification TLV, including the common address and device type. **identifier** *id* specifies the civic address policy ID. The value ranges from 1 to 1024. You must first configure the LLDP civic address, and then configure the device to allow the TLV to be advertised. **location elin identifier** *id*: indicates the emergency telephone number to be encapsulated in the Location Identification TLV. **identifier** *id*: indicates the emergency telephone number configured in a policy of a specified ID. The value ranges from 1 to 1024. You must first configure the emergency telephone number, and then configure the device to allow the TLV to be advertised. **network-policy profile** [*profile-number*]: indicates the network policy TLV, notifying the VLAN configuration of the interface, supported application types (such as voice or video), Layer 2 or Layer 3 priority information, and other items. *profile-number* specifies the network policy ID. The value ranges from 1 to 1024. If the device is connected to the downstream IP phone that supports LLDP-MED, you can configure the network policy TLV to deliver policies to the IP phone. You must first configure the network policy TLV, and then configure the device to allow the TLV to be advertised. **power-over-ethernet**: indicates the Extended Power-via-MDI TLV, that is, extended power supply capability.
Defaults	By default, an interface advertises all LLDP-MED TLVs except the Location Identification TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring an Interface Not to Advertise 802.1 TLVs

Configuration Steps	Cancel the advertisement of the IEEE 802.1 organizationally specific Port And Protocol VLAN ID TLV.
	Hostname(config)#interface gigabitethernet 0/1

	Hostname(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
Verification	Display LLDP TLV configuration in interface configuration mode.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1 LLDP tlv-config of port [GigabitEthernet 0/1] NAME STATUS DEFAULT ------ ------ ------- Basic optional TLV: Port Description TLV YES YES System Name TLV YES YES System Description TLV YES YES System Capabilities TLV YES YES Management Address TLV YES YES IEEE 802.1 extend TLV: Port VLAN ID TLV YES YES Port And Protocol VLAN ID TLV NO YES VLAN Name TLV YES YES IEEE 802.3 extend TLV: MAC-Physic TLV YES YES Power via MDI TLV YES YES Link Aggregation TLV YES YES Maximum Frame Size TLV YES YES LLDP-MED extend TLV: Capabilities TLV YES YES Network Policy TLV YES YES Location Identification TLV NO NO Extended Power via MDI TLV YES YES Inventory TLV YES YES

1.4.4 Configures the Management Address to Be Advertised

Configuration Effect

- Configure the management address to be advertised in LLDPDUs in interface configuration mode.
- After the management address to be advertised is cancelled, the management address in LLDPDUs 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 LLDPDUs in interface configuration mode.

↘ Configuring the Management Address to Be Advertised

Command	**lldp management-address-tlv** *ip-address*
Parameter Description	*ip-address*: specifies the management address to be advertised in an LLDPDU.
Defaults	A management address is advertised through LLDPDUs by default. The management address is the IPv4 address of the minimum VLAN supported by an interface. If no IPv4 address is configured for the VLAN, the device continues query until it finds the appropriate IPv4 address. If no IPv4 address is found, the device searches for the IPv6 address of the minimum VLAN supported by an interface. If no IPv6 address is found, the local address 127.0.0.1 is used as the management address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

Display LLDP information on a local interface

- Check whether the configuration takes effect.

Related Commands

↘ Configuring the Management Address to Be Advertised

Command	**no lldp management-address-tlv** [*ip-address*]
Parameter Description	**ip-address**: specifies the management address to be advertised in an LLDPDU.
Defaults	A management address is advertised through LLDPDUs by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port.

	If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Management Address to Be Advertised

Configuration Steps	Set the management address to 192.168.1.1 on an interface.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
Verification	Display configuration on the interface.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1 Lldp local-information of port [GigabitEthernet 0/1] Port ID type : Interface name Port id : GigabitEthernet 0/1 Port description : GigabitEthernet 0/1 Management address subtype : ipv4 Management address : 192.168.1.1 Interface numbering subtype : ifIndex Interface number : 1 Object identifier : 802.1 organizationally information Port VLAN ID : 1 Port and protocol VLAN ID(PPVID) : 1 PPVID Supported : YES PPVID Enabled : NO VLAN name of VLAN 1 : VLAN0001 Protocol Identity : 802.3 organizationally information

	Auto-negotiation supported : YES Auto-negotiation enabled : YES PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode Operational MAU type : speed(100)/duplex(Full) PoE support : NO Link aggregation supported : YES Link aggregation enabled : NO Aggregation port ID : 0 Maximum frame Size : 1500 LLDP-MED organizationally information Power-via-MDI device type : PD Power-via-MDI power source : Local Power-via-MDI power priority : Power-via-MDI power value : Model name : Model name

1.4.5 Configuring the LLDP Fast Transmission Count

Configuration Effect

- Configure the number of LLDPDUs that are fast transmitted.

Configuration Steps

- Optional.
- Configure the number of LLDPDUs that are fast transmitted in global configuration mode.

↘ Configuring the Number of LLDPDUs That Can Be Transmitted Rapidly

Command	**lldp fast-count** *fast-count-value*
Parameter Description	*fast-count-value*: indicates the number of LLDPDUs that are fast transmitted. The value ranges from 1 to 10.
Defaults	By default, three LLDPDUs are transmitted rapidly.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Displaying the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Restoring the Default LLDP Fast Transmission Count

Command	no lldp fast-count
Parameter Description	N/A
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the LLDP Fast Transmission Count

Configuration Steps	Set the LLDP fast transmission count to 5 in global configuration mode.
	Hostname(config)#lldp fast-count 5
Verification	Display the global LLDP status information.
	Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 5

1.4.6 Configuring the TTL Multiplier and Transmission Interval

Configuration Effect

- Configure the TTL multiplier.
- Configure the LLDP packet transmission interval.

Notes

- The LLDPDU transmission interval ranges from 1 to 32768, which is larger than the standard MIB range (5 to 32768). Therefore, this parameter can apply to more scenarios.

Configuration Steps

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

Configuring the TTL Multiplier

Command	**lldp hold-multiplier** *ttl-value*
Parameter Description	*ttl-value*: indicates the TLL multiplier. The value ranges from 2 to 10.
Defaults	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 LLDPDUs by configuring the TTL multiplier.

Configuring the LLDPDU Transmission Interval

Command	**lldp timer tx-interval** *tx-interval*
Parameter Description	*tx-interval*: indicates the LLDP packet transmission interval. The value ranges from 1 to 32,768.
Defaults	The default value is 30.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Restoring the Default TTL Multiplier

Command	**no lldp hold-multiplier**
Parameter Description	N/A
Defaults	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 LLDPDUs by configuring the TTL multiplier.

Restoring the Default Transmission Interval

Command	**no lldp timer tx-interval**

Parameter Description	N/A
Defaults	The default value is 30.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the TTL Multiplier

Configuration Steps	Set the TTL multiplier to 3 and the transmission interval to 20 seconds. The TTL of local device information on neighbors is 61 seconds.
	Hostname(config)#lldp hold-multiplier 3 Hostname(config)#lldp timer tx-interval 20
Verification	Display the global LLDP status information.
	Hostname(config)#lldp hold-multiplier 3 Hostname(config)#lldp timer tx-interval 20 Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 20s Hold multiplier : 3 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

1.4.7 Configuring the Transmission Delay

Configuration Effect

- Configure the delay time for LLDP packet transmission.

Configuration Steps

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

Configuring the Transmission Delay

Command	**lldp timer tx-delay** *tx-delay*
Parameter Description	*tx-delay*: indicates the transmission delay. The value ranges from 1 to 8,192.
Defaults	The default value is 2.
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDPDUs to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDPDUs caused by frequent changes of local information.

Verification

- Display the global LLDP status to check whether the configuration takes effect.

Related Commands

Restoring the Default LLDPDU Transmission Delay

Command	**no lldp timer tx-delay**
Parameter Description	N/A
Defaults	The default value is 2.
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDPDUs to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDPDUs caused by frequent changes of local information.

Configuration Example

Configuring the Transmission Delay

Configuration Steps	Set the transmission delay to 3 seconds.
	Hostname(config)#lldp timer tx-delay 3
Verification	Display the global LLDP status information.
	Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 3s

	Notification interval : 5s Fast start counts : 3

1.4.8 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.

↘ **Configuring the Initialization Delay**

Command	**lldp timer reinit-delay** *reinit-delay*
Parameter Description	*reinit-delay*: indicates the initialization delay. The value ranges from 1 to 10 seconds.
Defaults	The default value is 2.
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 working mode.

Verification

Display the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

↘ **Restoring the Default Initialization Delay**

Command	**no lldp timer reinit-delay**
Parameter Description	N/A
Defaults	The default value is 2.
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 working mode.

Configuration Example

↘ **Configuring the Initialization Delay**

Configuration Steps	Set the initialization delay to 3 seconds.
	Hostname(config)#lldp timer reinit-delay 3
Verification	Display the global LLDP status information.
	Hostname(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 3s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

1.4.9 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.

Command	**lldp notification remote-change enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance

↘ Configuring the LLDP Trap Transmission Interval

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

Command	**lldp timer notification-interval** *trap*
Parameter Description	*trap*: indicates the interval for transmitting LLDP Trap messages. The value ranges from 5 to 3,600 seconds.
Defaults	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.

Verification

Display LLDP status information

- Check whether the LLDP Trap function is enabled.
- Check whether the interval configuration takes effect.

Related Commands

↘ Disabling the LLDP Trap Function

Command	**no lldp notification remote-change enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
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.

↘ Restores the default LLDP trap transmission interval.

Command	**no lldp timer notification-interval**
Parameter Description	N/A
Defaults	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.

Configuration Example

↘ Enabling the LLDP Trap Function and Configuring the LLDP Trap Transmission Interval

Configuration Steps	Enable the LLDP Trap function and set the LLDP Trap transmission interval to 10 seconds.

	Hostname(config)#lldp timer notification-interval 10 Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Verification	Display LLDP status information.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 10s Fast start counts : 3 --- Port [GigabitEthernet 0/1] --- Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : YES Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

1.4.10 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.

Enabling the LLDP Error Detection Function

Command	**lldp error-detect**
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDPDUs exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Verification

Display LLDP status information on an interface

- Check whether the configuration takes effect.

Related Commands

Disabling the LLDP Error Detection Function

Command	**no lldp error-detect**
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDPDUs exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Configuration Example

Enabling the LLDP Error Detection Function

Configuration Steps	Enable the LLDP error detection function on interface GigabitEthernet 0/1.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp error-detect
Verification	Display LLDP status information on the interface.

	Hostname(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

1.4.11 Configuring the LLDP Encapsulation Format

Configuration Effect

- Configure the LLDP encapsulation format.

Configuration Steps

- Optional.
- Configure the LLDP encapsulation format on an interface.

Setting the LLDP Encapsulation Format to SNAP

Command	**lldp encapsulation snap**
Parameter Description	N/A
Defaults	The LLDP encapsulation format is Ethernet II.
Command Mode	Interface configuration mode
Usage Guide	⚠ The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Verification

Display LLDP status information of an interface

- Check whether the configuration takes effect.

Related Commands

Restoring the Default LLDP Encapsulation Format (Ethernet II)

Command	**no lldp encapsulation snap**

Parameter Description	N/A
Defaults	The LLDP encapsulation format is Ethernet II.
Command Mode	Interface configuration mode
Usage Guide	⚠ The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Configuration Example

↘ Setting the LLDP Encapsulation Format to SNAP

Configuration Steps	Set the LLDP encapsulation format to SNAP.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
Verification	Display LLDP status information on the interface.
	Hostname(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Snap Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

1.4.12 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:
  - (a) Enable the voice VLAN function and add the port connected to the IP phone to the voice VLAN.
  - (b) Configure the port connected to the IP phone as a QoS trusted port (the trusted DSCP mode is recommended).

(c) 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 details on how to configure the QoS trust mode, see *Configuring QoS*. For details on how to configure a secure channel, see *Configuring ACL*.

Configuration Steps

- Optional.
- Configure the LLDP network policy.

Configuring the LLDP Network Policy

Command	**lldp network-policy profile** *profile-num*
Parameter Description	*profile-num*: indicates the ID of an LLDP network policy. The value ranges from 1 to 1,024.
Defaults	LLDP network policy is not configured by default.
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.

Configuring the Voice VLAN Policy

Command	{ **voice** | **voice-signaling** } **vlan** { { { *vlan-id* | **dot1p** } [**cos** *cos* | **dscp** *dscp*] } | **untagged** | **none** }
Parameter Description	**voice**: Voice application. **voice-signaling**: Voice-signaling application. *vlan-id*: The tagged frame is sent in the voice VLAN in VoIP. The tagged frame includes **user_priority** and **vlan id**. The VLAN ID of voice flow ranges from 1 to 4094. **dot1p**: The tagged frame is sent in the voice VLAN in VoIP. The tagged frame includes **user_priority** and **vlan id** is 0. **cos** *cos*: The tagged frame is sent in the voice VLAN in VoIP. The CoS value of the voice flow ranges from 0 to 7. The default value is 5. **dscp** *dscp*: The tagged frame is sent in the voice VLAN in VoIP. The Differentiated Services Code Point (DSCP) value of the voice flow ranges from 0 to 63. The default value is 46. **untagged**: The network policy is not advertised. VoIP determines the network policy based on its configuration. **none**: The untagged frame is sent in the voice VLAN in VoIP. In this case, the value of *vlan id* and *cos* are ignored.
Defaults	The voice VLAN policy is not configured by default.
Command Mode	LLDP network policy mode
Usage Guide	N/A

Configuring an Interface to Advertise an LLDP Network Policy

Command	**lldp tlv-enable med-tlv network-policy profile** [*profile-num*]
Parameter Description	**network-policy profile** [*profile-number*]: indicates the network policy TLV, notifying the VLAN configuration of the interface, supported application types (such as voice or video), Layer 2 or Layer 3 priority information, and other items. *profile-number* specifies the network policy ID. The value ranges from 1 to 1024. If the device is connected to the downstream IP phone that supports LLDP-MED, you can configure the network policy TLV on the device to deliver policies to the IP phone. You must first configure the network policy TLV, and then configure the device to allow the TLV to be advertised.
Defaults	The network policy TLV can be advertised on an interface.
Command Mode	Interface configuration mode
Usage Guide	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.

Verification

Displaying the LLDP network policy configuration.

- Check whether the configuration takes effect.

Related Commands

Deleting the LLDP Network Policy

Command	**no lldp network-policy profile** *profile-num*
Parameter Description	*profile-num*: indicates the LLDP network policy ID. The value ranges from 1 to 1,024.
Defaults	LLDP network policy is not configured by default.
Command Mode	Interface configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the { **voice** | **voice-signaling** } **vlan** command to configure a specific network policy.

Deleting the Voice VLAN Policy

Command	**no** { **voice** | **voice-signaling** } **vlan**
Parameter Description	**voice**: Voice application. **voice-signaling**: Voice-signaling application.
Defaults	The voice VLAN policy is not configured by default
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring an Interface Not to Advertise an LLDP Network Policy

Command	**no lldp tlv-enable med-tlv network-policy profile** [*profile-num*]
Parameter Description	**network-policy profile** [*profile-number*]: indicates the network policy TLV, notifying the VLAN configuration of the interface, supported application types (such as voice or video), Layer 2 or

	Layer 3 priority information, and other items. *profile-number* specifies the network policy ID. The value ranges from 1 to 1024. If the device is connected to the downstream IP phone that supports LLDP-MED, you can configure the network policy TLV on the device to deliver policies to the IP phone. You must first configure the network policy TLV, and then configure the device to allow the TLV to be advertised.
Defaults	The network policy TLV can be advertised on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the LLDP Network Policy

Configuration Steps	Configure the network policy TLV for LLDPDUs to be advertised by GigabitEthernet 0/1 and configure policy 1. In the policy, set the VLAN ID of the voice application to 3, CoS value to 4, and DSCP priority to 6. LLDPDUs
	Hostname#config Hostname(config)#lldp network-policy profile 1 Hostname(config-lldp-network-policy)# voice vlan 3 cos 4 Hostname(config-lldp-network-policy)# voice vlan 3 dscp 6 Hostname(config-lldp-network-policy)#exit Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
Verification	Display the LLDP network policy configuration on the local device.
	network-policy information: --- network policy profile :1 voice vlan 3 cos 4 voice vlan 3 dscp 6

1.4.13 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.

Configuring the Common Address of a Device

Command	**lldp location civic-location identifier** *id*
Parameter Description	*id*: indicates the ID of a common address of a network device, in the range from 1 to 1024.
Defaults	The common address of a device is not configured by default.
Command Mode	Global configuration mode
Usage Guide	This command is used to create an LLDP civic address and enter the LLDP civic address configuration mode. After entering the LLDP civic address configuration mode, configure the LLDP common address.

Configuring the Civic Address of a Device

Command	Configure the LLDP civic address. Use the **no** option to delete the address. { **country** | **state** | **county** | **city** | **division** | **neighborhood** | **street-group** | **leading-street-dir** | **trailing-street-suffix** | **street-suffix** | **number** | **street-number-suffix** | **landmark** | **additional-location-information** | **name** | **postal-code** | **building** | **unit** | **floor** | **room** | **type-of-place** | **postal-community-name** | **post-office-box** | **additional-code** } *ca-word*
Parameter Description	**country**: indicates the country code, with two characters. CH indicates China. **state**: indicates the CA type is 1. **county**: indicates that the CA type is 2. **city**: indicates that the CA type is 3. **division**: indicates that the CA type is 4. **neighborhood**: indicates that the CA type is 5. **street-group**: indicates that the CA type is 6. **leading-street-dir**: indicates that the CA type is 16. **trailing-street-suffix**: indicates that the CA type is 17. **street-suffix**: indicates that the CA type is 18. **number**: indicates that the CA type is 19. **street-number-suffix**: indicates that the CA type is 20. **landmark**: indicates that the CA type is 21. **additional-location-information**: indicates that the CA type is 22. **name**: indicates that the CA type is 23. **postal-code**: indicates that the CA type is 24. **building**: indicates that the CA type is 25. **unit**: indicates that the CA type is 26. **floor**: indicates that the CA type is 27. **room**: indicates that the CA type is 28. **type-of-place**: indicates that the CA type is 29. **postal-community-name**: indicates that the CA type is 30. **post-office-box**: indicates that the CA type is 31. **additional-code**: indicates that the CA type is 32. *ca-word*: indicates the address.
Defaults	The common address of a device is not configured by default.

Command Mode	LLDP civic address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Configuring the Device Type

Command	**device-type** *device-type*
Parameter Description	*device-type*: indicates the device type. The value ranges from 0 to 2. The default value is 1. The value 0 indicates that the device type is DHCP server. The value 1 indicates that the device type is switch. The value indicates that the device type is LLDP MED .
Defaults	The device type is not configured by default.
Command Mode	LLDP civic address configuration mode
Usage Guide	After entering the LLDP civic address configuration mode, configure the device type.

Configuring the Civic Address in Location Identification TLV to Be Advertised

Command	**lldp tlv-enable med-tlv location civic-location identifier** *id*
Parameter Description	**med-tlv**: indicates the LLDP MED TLV. **location**: indicates the Location Identification TLV. **civic-location**: indicates the civic address information and postal information. **identifier** *id*: indicates the policy ID, ranging from 1 to 1,024.
Defaults	The Location Identification TLV cannot be advertised on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Display the LLDP civic address of the local device to check whether the configuration takes effect.

Related Commands

Restoring the Default LLDP Civic Address

Command	**no lldp location civic-location identifier** *id*
Parameter Description	*id*: indicates the ID of a common address of a network device, in the range from 1 to 1024.
Defaults	The common address of a device is not configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default Common Address of the 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
Defaults	The common address of a device is not configured by default.
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Restoring the Default Device Type

Command	**no device-type**
Parameter Description	N/A
Defaults	The default device ID is 1, that is, switch.
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, restore the default settings.

Configuring the Interface Not to Advertise the Civic Address

Command	**no lldp tlv-enable med-tlv location civic-location identifier** *id*
Parameter Description	**med-tlv**: indicates the LLDP MED TLV. **location**: indicates the Location Identification TLV. **civic-location**: indicates the civic address information and postal information. **identifier** *id*: indicates the policy ID, ranging from 1 to 1,024.
Defaults	The Location Identification TLV cannot be advertised on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Civic Address of a Device

Configuration Steps	Configure GigabitEthernet 0/1 to advertise the civic address. Set the device type to switch, country to Thailand, city to Bangkok, and postal code to 999003.
	Hostname# config Hostname(config)# lldp location civic-location identifier 1 Hostname(config-lldp-civic)# country Thailand Hostname(config-lldp-civic)# city Bangkok Hostname(config-lldp-civic)# postal-code 999003 Hostname(config-lldp-civic)# exit Hostname(config)# interface gigabitethernet 0/1

	Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv location civic-location identifier 1
Verification	Check the LLDP common address of GigabitEthernet 0/1.
	Hostname# show lldp location civic-location identifier 1 civic location information: ---------- Identifier :1 country :Thailand device type :1 city :Bangkok postal-code :999003

1.4.14 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.

↘ Configuring the Emergency Telephone Number of a Device

Command	**lldp location elin identifier** *id* **elin-location** *tel-number*
Parameter Description	*id*: indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024. *tel-number*: indicates the emergency telephone number, containing 10-25 characters.
Defaults	The emergency telephone number of a device is not configured by default.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the emergency telephone number.

↘ Configuring the Emergency Telephone Number in Location Identification TLV to Be Advertised

Command	**lldp tlv-enable med-tlv location elin identifier** *id*
Parameter Description	**med-tlv**: indicates the LLDP MED TLV. **location**: indicates the Location Identification TLV. **elin**: indicates the emergency telephone number. **identifier** *id*: indicates the policy ID, ranging from 1 to 1,024.
Defaults	The Location Identification TLV cannot be advertised on an interface.

Command Mode	Interface configuration mode
Usage Guide	You must first configure the emergency telephone number, and then configure the device to allow the TLV to be advertised.

Verification

Display the emergency telephone number of the local device

- Check whether the configuration takes effect.

Related Commands

Deleting the Emergency Telephone Number of a Device

Command	**no lldp location elin identifier** *id*
Parameter Description	*id*: indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024.
Defaults	The emergency telephone number of a device is not configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Canceling the Emergency Telephone Number in Location Identification TLV

Command	**no lldp tlv-enable med-tlv location elin identifier** *id*
Parameter Description	**med-tlv**: indicates the LLDP MED TLV. **location**: indicates the Location Identification TLV. **elin**: indicates the emergency telephone number. **identifier** *id*: indicates the policy ID, ranging from 1 to 1024.
Defaults	The Location Identification TLV cannot be advertised on an interface.
Command Mode	Interface configuration mode
Usage Guide	You must first configure the emergency telephone number, and then configure the device to allow the TLV to be advertised.

Configuration Example

Configuring the Emergency Telephone Number of a Device

Configuration Steps	Configure the emergency telephone numbers issued by GigabitEthernet 0/1 and GigabitEthernet 0/2 to 085283671111 and 085283671112, respectively.
	Hostname#config Hostname(config)#lldp location elin identifier 1 elin-location 085283671111 Hostname(config)#lldp location elin identifier 2 elin-location 085283671112 Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv location elin identifier 1 Hostname(config-if-GigabitEthernet 0/1)# exit Hostname(config)# interface gigabitethernet 0/2

	Hostname(config-if-GigabitEthernet 0/2)# lldp tlv-enable med-tlv location elin identifier 2 Hostname(config-if-GigabitEthernet 0/2)# end
Verification	Check the emergency telephone numbers issued by GigabitEthernet 0/1 and GigabitEthernet 0/2.
	Hostname# show lldp location elin-location interface gigabitethernet 0/1 elin location information: ---------- Identifier :1 elin number :085283671111 Hostname# show lldp location elin-location interface gigabitethernet 0/2 elin location information: ---------- Identifier :2 elin number :085283671112

1.4.15 Configuring the Function of Ignoring PVID Detection

Configuration Effect

- Ignores the PVID detection.

Configuration Steps

- Optional.
- According to the real condition, select whether to enable the function.

↘ Ignoring PVID Detection

Command	**lldp ignore pvid-error-detect**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Use the command to ignore PVID detection.

Verification

Display the LLDP information.

- Check whether the status of PVID detection in global LLDP is the same as your configuration.

Related Commands

↘ Ignoring PVID Detection

Command	**no lldp ignore pvid-error-detect**
Parameter Description	N/A

Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Function of Ignoring PVID Detection

Configuration Steps	Ignores PVID detection in global configuration mode.
	Hostname# config Hostname(config)# lldp ignore pvid-error-detect
Verification	Display the LLDP information.
	Hostname# 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 Igore PVID error detect : YES

1.5 Monitoring

Clearing

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

Description	Command
Clears LLDP statistics.	**clear lldp statistics** [**interface** *interface-type interface-number*]
Clears LLDP neighbor information.	**clear lldp table** [**interface** *interface-type interface-number*]

Displaying

Description	Command
Displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.	**show lldp local-information** [**global** | **interface** *interface-type interface-number*]
Displays the LLDP civic address or emergency telephone number of a local device.	**show lldp location** { **civic-location | elin-location** } { **identifier** *id* **| interface** *interface-type interface-number* | **static** }
Displays LLDP information on a neighbor.	**show lldp neighbors** [**interface** *interface-type interface-number*] [**detail**]
Displays the LLDP network policy configuration of the local device.	**show lldp network-policy** { **profile** [*profile-num*] | **interface** *interface-type interface-number* }
Displays LLDP statistics.	**show lldp statistics** [**global** | **interface** *interface-type interface-number*]
Displays LLDP status information.	**show lldp status** [**interface** *interface-type interface-number*]
Displays the configuration of TLVs to be advertised by a port.	**show lldp tlv-config** [**interface** *interface-type interface-number*]

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**

Configuring IP Service

1. Configuring ARP
2. Configuring Proxy ARP
3. Configuring IPv4 Basics
4. Configuring NAT
5. Configuring DHCP
6. Configuring DHCP Snooping
7. Configuring DNS
8. Configuring DNS SNOOPING
9. Configuring IPv6 Basics
10. Configuring DHCPv6
11. Configuring ND Proxy
12. Configuring TCP
13. Configuring IP REF
14. Configuring FPM

1 Configuring ARP

1.1 Overview

In a local area network (LAN), each IP network device has two addresses: 1) local address. Since the local address is contained in the header of the data link layer (DLL) frame, it is a DLL address. However, it is processed by the MAC sublayer at the DLL and thereby is usually called the MAC address. MAC addresses represent IP network devices on LANs. 2) network address. Network addresses on the Internet represent IP network devices and also indicate the networks where the devices reside.

In a LAN, two IP devices can communicate with each other only after they learn the 48-bit MAC address of each other. The process of obtaining the MAC address based on the IP address is called address resolution. There are two types of address resolution protocols: 1) Address Resolution Protocol (ARP); 2) Proxy ARP. ARP and Proxy ARP are described respectively in RFC 826 and RFC 1027.

ARP is used to bind the MAC address with the IP address. When you enter an IP address, you can learn the corresponding MAC address through ARP. Once the MAC address is obtained, the IP-MAC mapping will be saved to the ARP cache of the network device. With the MAC address, the IP device can encapsulate DLL frames and send them to the LAN. By default, IP and ARP packets on the Ethernet are encapsulated in Ethernet II frames.

Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

1.2 Applications

Application	Description
LAN-based ARP	A user learns the MAC addresses of other users in the same network segment through ARP.

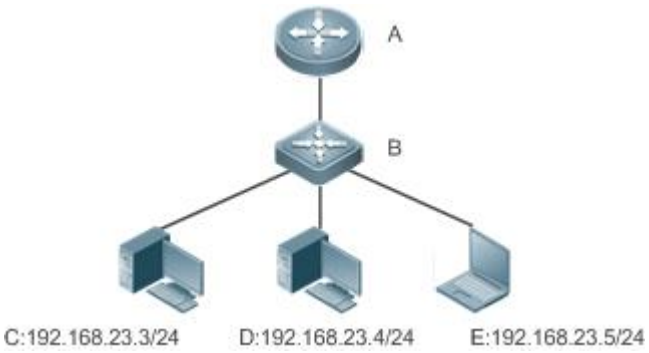
1.2.1 LAN-based ARP

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 1-1



Remarks	A is the router. B is the gateway of the network segment where terminals reside. C, D, and E are hosts.

Deployment

- Enable ARP in a LAN to implement IP-MAC mapping.

1.3 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.
ARP Packet Statistics Collection	Displays ARP statistics.

1.3.1 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.

1.3.2 ARP Attributes

Users can specify the ARP timeout, ARP request retransmission interval and times, and maximum number of unresolved ARP entries.

Working Principle

ARP Timeout

The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP entry timeout expires, the device sends a unicast ARP request packet to detect whether the peer end is online. If it receives an ARP reply from the peer end, it does not delete this ARP entry. Otherwise, the device deletes this ARP entry.

When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth.

ARP Request Retransmission Interval and Times

The device consecutively sends ARP requests to resolve an IP address to a MAC address. The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request is retransmitted, the more likely the resolution will succeed and the more bandwidth ARP will consume.

Maximum Number of Unresolved ARP Entries

In a LAN, ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the users. To prevent such attacks, users can configure the maximum number of unresolved ARP entries.

Related Configuration

Configuring the ARP Timeout

Run the **arp timeout** *seconds* command in interface configuration mode to configure the ARP timeout. The default timeout is 3,600 seconds. You can change it based on actual situations.

Configuring the ARP Request Retransmission Interval and Times

- Run the **arp retry interval** *seconds* command in global configuration mode to configure the ARP request retransmission interval. The default interval is 1 second. You can change it based on actual situations.
- Run the **arp retry times** *number* command in global configuration mode to configure the ARP request retransmission times. The default number of retransmission times is 5. You can change it based on actual situations.

Configuring the Maximum Number of Unresolved ARP Entries

Run the **arp unresolve** *number* command in global configuration mode to configure the maximum number of unresolved ARP entries. The default value is the maximum number of ARP entries supported by the device. You can change it based on actual situations.

1.3.3 ARP Packet Statistics Collection

Working Principle

The device counts the total number of ARP request and reply packets sent and received by each interface, and packets of unknown types on all interfaces from power-on.

1.4 Configuration

Configuration	Description and Command	
Enabling Static ARP	(Optional) It is used to enable static IP-MAC binding.	
	arp	Enables static ARP.
Configuring ARP Attributes	⚠ (Optional) It is used to specify the ARP timeout, ARP request retransmission interval and times, and maximum number of unresolved ARP entries.	
	arp timeout	Configures the ARP timeout.
	arp retry interval	Configures the ARP request retransmission interval.
	arp retry times	Configures the local retry times of the ARP request message.
	arp unresolve	Configures the maximum number of unresolved ARP entries.

1.4.1 Enabling Static ARP

Configuration Effect

Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.

Notes

After a static ARP entry is configured, the Layer-3 switch learns the physical port corresponding to the MAC address in the static ARP entry before it performs Layer-3 routing.

Configuration Steps

↘ Configuring Static ARP Entries

- Optional.
- You can configure a static ARP entry to bind the IP address of the uplink device with its MAC address to prevent MAC change caused by ARP attacks.
- Configure static ARP entries in global configuration mode.

Verification

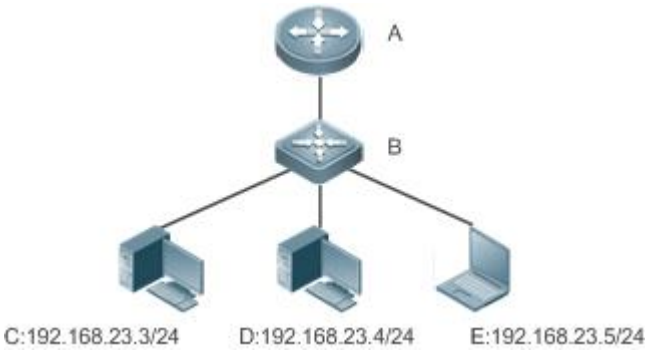
Run the **show running-config** command to check whether the configuration takes effect. Or run the **show arp static** command to check whether a static ARP cache table is created.

Related Commands

↘ Configuring Static ARP Entries

Command	arp [vrf name | oob] ip-address mac-address type
Parameter Description	ip-address: Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format. mac-address Indicates the DLL address, consisting of 48 bits. type Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.
Command Mode	Global configuration mode
Usage Guide	The 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.

Configuration Example

Scenario	 Note: A is the router. B is the gateway of the network segment where terminals reside. C, D, and E are terminals.
Configuration Steps	Configure a static ARP entry on B to statically bind the IP address of A with the MAC address. `Hostname(config)# ap-group 00D0.F822.334B-ap`

Verification	Run the **show arp static** command to display the static ARP entry.
	`Hostname#show arp static`
	`Protocol Address Age(min) Hardware Type Interface`
	`Internet 192.168.23.1 <static> 00D0.F822.334B arpa`
	`1 static arp entries exist.`

Common Errors

- The MAC address in static ARP is incorrect.

1.4.2 Configuring ARP Attributes

Configuration Effect

Users can specify the ARP timeout, ARP request retransmission interval and times, and maximum number of unresolved ARP entries.

Configuration Steps

↘ Configuring the ARP Timeout

- Optional.
- In a LAN, if a user goes online/offline frequently, it is recommended to set the ARP timeout small to delete invalid ARP entries as soon as possible.
- Configure the ARP timeout in interface configuration mode.

↘ Configuring the ARP Request Retransmission Interval and Times

- Optional.
- If the network resources are insufficient, it is recommended to set the ARP request retransmission interval great and the retransmission times small to reduce the consumption of network bandwidths.
- Configure the ARP request retransmission interval and times in global configuration mode.

↘ Configuring the Maximum Number of Unresolved ARP Entries

- Optional.
- If the network resources are insufficient, it is recommended to set the maximum number of unresolved ARP entries small to reduce the consumption of network bandwidths.
- Configure the maximum number of unresolved ARP entries in global configuration mode.

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 unresolved ARP entries.

Related Commands

↘ Configuring the ARP Timeout

Command	**arp timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout in seconds, ranging from 0 to 2,147,483. The default value is 3,600.
Command Mode	Interface configuration mode
Usage Guide	The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. Unless otherwise specified, do not configure the ARP timeout.

Configuring the ARP Request Retransmission Interval

Command	**arp retry interval** *seconds*
Parameter Description	*seconds*: Indicates the ARP request retransmission interval in seconds, ranging from 1 to 3,600. The default value is 1.
Command Mode	Global configuration mode
Usage Guide	If a device frequently sends ARP requests, affecting network performance, you can set the ARP request retransmission interval longer. Ensure that this interval does not exceed the ARP timeout.

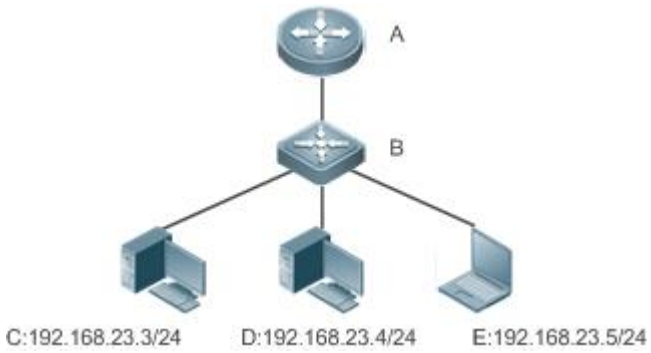
Configuring the Local Retry Times of the ARP Request Message

Command	**arp retry times** *number*
Parameter Description	number: indicates the number of transmission times of an ARP request. The value ranges from 1 to 100. When the value is set to **1**, an ARP request is sent once, and will not be retransmitted. The default value is **5**.
Command Mode	Global configuration mode
Usage Guide	When the device frequently sends ARP packets, problems such as network congestion may occur. you can set retransmission count of an ARP request to a smaller value.

Configuring the Maximum Number of Unresolved ARP Entries

Command	**arp unresolve** *number*
Parameter Description	number indicates the maximum number of unresolved ARP entries, ranging from 1 to 8,192. The default value is **8192**.
Command Mode	Global configuration mode
Usage Guide	If a large number of unresolved entries exist in the ARP cache table and remain in the table after a while, it is recommended to use this command to limit the number of unresolved ARP entries. ⚠ The maximum number of unresolved ARP entries limits the number of neighbor addresses that can be resolved at a time. If the device needs to resolve a large number of neighbor addresses, the neighbor addresses exceeding the limit will be resolved after existing neighbor addresses are resolved or the resolution time is reached. The resolution time of all neighbor addresses is longer when the maximum number of unresolved ARP entries is not set. Set the maximum number as required.

Configuration Example

Scenario	 Note: A is the router. B is the gateway of the network segment where terminals reside. C, D, and E are terminals.
Configuration Steps	● Set the ARP timeout to 60 seconds on port GigabitEthernet 0/1. ● Set the ARP request retransmission interval to 3 seconds. ● Set the ARP request retransmission times to 4. ● Set the maximum number of unresolved ARP entries to 4,096.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#arp timeout 60 Hostname(config-if-GigabitEthernet 0/1)#exit Hostname(config)#arp retry interval 3 Hostname(config)#arp retry times 4 Hostname(config)#arp unresolve 4096
Verification	● 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 unresolved ARP entries.
	Hostname#show arp timeout ---------- ---------- GigabitEthernet 0/1 60 GigabitEthernet 0/2 3600 GigabitEthernet 0/4 3600 GigabitEthernet 0/5 3600 GigabitEthernet 0/7 3600 VLAN 100 3600 VLAN 111 3600 Mgmt 0 3600 Ruijie(config)# show running-config

	Hostname# show running-config arp retry times 4 arp retry interval 3 arp dynamic-entry-limit 1 2 1000 interface GigabitEthernet 0/1

1.5 Monitoring

Clearing

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

Description	Command
Clears dynamic ARP entries. In gateway authentication mode, dynamic ARP entries in authentication VLANs are not cleared.	**clear arp-cache**

Displaying

Description	Command
Displays the ARP table.	**show arp** [*interface-type interface-number* [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]
Displays the ARP table.	**show ip arp**
Displays the ARP entry counter.	**show arp counter**
Displays the timeout of dynamic ARP entries.	**show arp timeout**
Displays ARP packet statistics.	**show arp packet statistics** [*interface*]

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**

1 Configuring ARP Proxy

1.1 Overview

ARP Proxy can work as a proxy for a device in the wireless local area network (WLAN) to respond to ARP requests of another device. Because CSMA/CA is used for communication in a wireless network, ARP Proxy can prevent ARP broadcast packets in one access point (AP) from being sent to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Protocols and Standards

N/A

1.2 Applications

Application	Description
ARP Proxy Service in the WLAN	AC acts as a proxy to respond to ARP requests of any device in the WLAN.

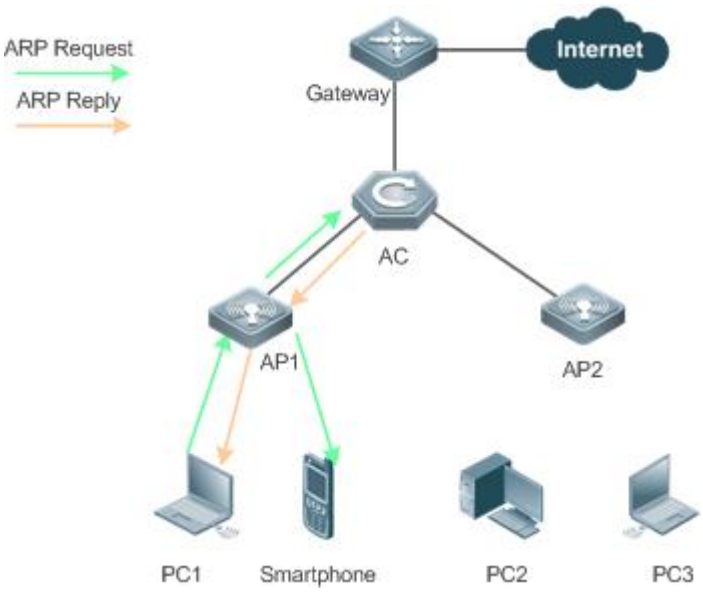
1.2.1 ARP Proxy Service in the WLAN

Scenario

In centralized forwarding mode of the fit AP, AC acts a proxy for ARP requests of any device in the WLAN.

- The AC needs to learn the MAC address of devices in the WLAN before responding to this device.

Figure 1-1



Remarks	The above figure is the flowchart of the ARP request packets that wireless STAs send to the gateway

	or other devices in centralized forwarding mode of the fit AP in the WLAN.

Deployment

- Deploy a network consisting of the gateway, AC, APs, and wireless STAs. Using the ARP Proxy function (enabled by default), AC works as a proxy to respond to the ARP requests of wireless STAs to prevent the ARP broadcast requests from being sent to other APs.
- The ARP Proxy runs on AC and is transparent to users. You can run this function without any other configurations. For details about how to deploy the network environment, refer to the chapter related to wireless networking.

1.3 Features

Basic Concepts

↘ ARP Proxy

Layer 2 ARP Proxy is also called ARP Proxy and works as a proxy for a device in the WLAN to respond to the ARP requests of another device. Because CSMA/CA is used for communication in a wireless network, ARP Proxy can prevent ARP broadcast packets in one AP from being sent to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Overview

Feature	Description
Wireless ARP Proxy	AC works as an ARP proxy for wireless STAs to prevent the ARP broadcast requests from being sent to other APs.

1.3.1 Wireless ARP Proxy

Working Principle

In typical wireless networking, a wireless STA usually accesses the Internet through an AP and AC. The typical scenario is that, multiple wireless STAs are associated with one AP while multiple APs are associated with one AC. When wireless STAs under one AP connect to those under another AP, or wireless STAs connect to wired STAs, or wired STAs connect to wireless STAs, ARP packets must be transmitted through AC, facilitating the implementation of AC's ARP Proxy function.

The working process of ARP Proxy is as follows:

1. AC learns the source IP address and source MAC address from the transmitted ARP packet to form an ARP entry.
2. According to the ARP entry, the AC works as a proxy in the network to respond to ARP requests of other users.
3. If the AC does not have the MAC address of the destination host, it forwards the 802.1Q-compliant ARP request.
4. ARP replies are forwarded like 802.1Q-compliant Ethernet frames.

As shown in Figure 1-1, PC3 and PC1 obtain the MAC address of the gateway respectively. Assume that this WLAN has one AC, two APs (AP1 and AP2), and four STAs (PC1, PC2, PC3 and smartphone).

1. PC3 initiates an ARP request to the IP address of the gateway.
2. AP2 forwards this ARP request to PC2 and AC.
3. From this ARP request, AC learns the IP and MAC address of PC3 and forwards this ARP request to the gateway, AP1, and PC1 and the smartphone under AP1.
4. The gateway sends an ARP reply to PC4 through AC. Then AC learns the IP and MAC address of the gateway.
5. PC1 initiates an ARP request to the IP address of the gateway.
6. AP1 forwards this ARP request to PC2 and AC.
7. AC learns the IP and MAC address of PC1 and works as a proxy for the gateway to directly send an ARP reply to PC1. (This is because AC has learned the MAC address of the gateway in step 4. Therefore, ARP request packets will not be broadcast to PC3 and PC4.)

Related Configuration

Enabling Layer 2 ARP Proxy

- By default, Layer 2 ARP Proxy is enabled.
- Run the **no proxy_arp enable** command to disable Layer 2 ARP Proxy.

1.4 Configuration

Configuration	Description and Command	
Enabling Layer 2 ARP Proxy	⚠ (Optional) By default, Layer 2 ARP Proxy is enabled.	
	proxy-arp enable	Enables Layer 2 ARP Proxy
Enabling Learning of Only ARP Entries on Wireless Ports	⚠ (Optional) By default, learning of only ARP entries over wireless ports is disabled.	
	proxy-arp learn only-wlan [**except** *ip-address*]	Enables learning of only ARP entries over wireless ports and ARP entries of special IP addresses over wired ports.

1.4.1 Enabling Layer 2 ARP Proxy

Configuration Effect

Enabling Layer 2 ARP Proxy improves wireless bandwidth efficiency and user experience.

Notes

N/A

Configuration Steps

Enabling Layer 2 ARP Proxy

- By default, Layer 2 ARP Proxy is enabled.
- In a wireless IPv4 scenario, enabling Layer 2 ARP Proxy on AC to better network bandwidth utilization and user experience.

Verification

Run the **show running-config** command to check whether Layer 2 ARP Proxy is enabled.

Related Commands

Disabling Layer 2 ARP Proxy

Command	**no proxy-arp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Disabling Layer 2 ARP Proxy

Configuration Steps	Disable Layer 2 ARP Proxy.
	Hostname(config)# no proxy-arp enable
Verification	Run the **show running-config** command to check if Layer 2 ARP Proxy is enabled.
	Hostname# show running-config no proxy-arp enable

Common Errors

N/A

1.4.2 Enabling Learning of Only ARP Entries on Wireless Ports

Configuration Effect

Enable learning of only ARP entries on wireless ports according to actual topologies. The device can learn special IP addresses on wired ports. In this way, ARP entry capacity on an AC will not be fully occupied by ARP packets on wired ports.

Notes

When the ARP entry capacity on a device is sufficient (To display the capacity, run **show proxy-arp statistic**.), it is recommended that this function be disabled. This is because when the ARP proxy learns ARP entries over wired ports, broadcast flooding of ARP entries requested from wired users can be prevented.

Configuration Steps

↘ Enabling Learning of Only ARP Entries over Wireless Ports

- By default, learning of only ARP entries over wireless ports is disabled and needs to be manually enabled as required.
- If the AC does not function as the gateway, you are advised to configure learning of ARP entries of special IP addresses at the same time when configuring learning of only ARP entries over wireless ports to learn the gateway IP address over wired ports.

Verification

- Run the **show running-config** command to check whether the configuration is correct.

Related Commands

↘ Enabling Learning of Only ARP Entries over Wireless Ports for an ARP Proxy

Command	**proxy-arp learn only-wlan** [**except** *ip_address*]
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This function can be enabled when the following conditions are met: 1) The AC works in integrated forwarding mode. 2) The AC interconnects with the gateway. The gateway interconnects with the switch. Configure a super VLAN and many sub-VLANs for STAs on the switch; 3) The user quantity is large, and therefore the capacity of ARP entries on the ARP proxy easily gets full. To check the capacity, run the **show proxy-arp statistics** command.

Configuration Example

↘ Enabling Learning of Only ARP Entries over Wireless Ports for an ARP Proxy

Configuration Steps	Enable learning of only ARP entries over wireless ports and ARP entries of IP addresses 192.168.21.1 and 192.168.22.1.
	Hostname(config)# proxy-arp learn only-wlan except 192.168.21.1 Hostname(config)# proxy-arp learn only-wlan except 192.168.22.1
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Hostname#show running-config

	proxy-arp learn only-wlan except 192.168.21.1 proxy-arp learn only-wlan except 192.168.22.1

1.5 Monitoring

Clearing

Description	Command
Clears the specified ARP Proxy entry.	**clear proxy-arp** [*ip-address vlan-id*]
Clears all ARP Proxy entries.	**clear proxy-arp**

Displaying

Description	Command
Displays all ARP Proxy entries.	**show proxy-arp** [*ip-address*]
Displays dynamic ARP Proxy entries.	**show proxy-arp dynamic**
Displays the ARP Proxy statistics.	**show proxy-arp statistics**

Debugging

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

Description	Command
Debugs the receipt/sending status of ARP packets.	**debug proxy-arp**

1 Configuring IPv4 Basics

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: AddressAllocationforPrivateInternets
- RFC 1166: Internet Numbers

1.2 Applications

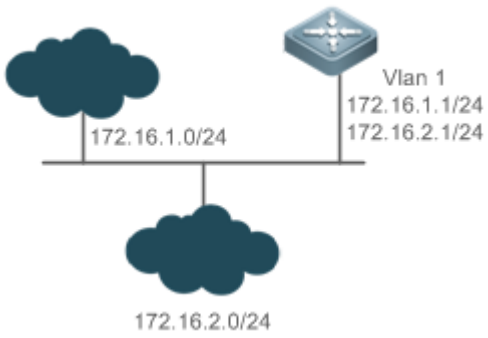
Application	Description
Configuring an IP Address for Communication	Two networks communicate through one interface.

1.2.1 Configuring an IP Address for Communication

Scenario

A device 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 device and computers between the two network segments can communicate with each other.

Figure 1-1 Configuring IP Addresses



Deployment

- Configure two IP addresses on VLAN1. One is a primary IP address and the other is a secondary IP address.
- On hosts in the network segment 172.16.1.0/24, set the gateway to 172.16.1.1; on hosts in the network segment 172.16.2.0/24, set the gateway to 172.16.2.1.

1.3 Features

Basic Concepts

IP Address

An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal. When expressed in decimal, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by a full stop ".". For example, "192.168.1.1" is an IP address expressed in decimal.

IP addresses are used for interconnection at the IP layer. A 32-bit IP address consists of two parts, namely, the network bits and the host bits. Based on the values of the first several bits in the network part, IP addresses in use can be classified into four classes.

For a class A address, the most significant bit is 0.7 bits indicate a network ID, and 24 bits indicate a local address. There are 128 class A networks in total.

Figure 1-2

		8	16 24 32
Class A IP address	0	Network ID	Host ID

For a class B address, the first two most significant bits are 10.14 bits indicate a network ID, and 16 bits indicate a local address. There are 16,348 class B networks in total.

Figure 1-3

			8	16 24 32
Class B IP address	1	0	Network ID	Host ID

For a class C address, the first three most significant bits are 110.21 bits indicate a network ID, and 8 bits indicate a local address. There are 2,097,152 class C networks in total.

Figure 1-4

				8	16 24 32
Class C IP address	1	1	0	Network ID	Host ID

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

Figure 1-5

					8	16 24 32
Class D IP	1	1	1	0	Multicast address	

address					

The addresses with the first four most significant bits 1111 cannot be assigned. These addresses are called class E addresses and are reserved.

When IP addresses are planned during network construction, IP addresses must be assigned based on the property of the network to be built. If the network needs to be connected to the Internet, users should apply for IP addresses to the corresponding agency. In China, you can apply to China Internet Network Information Center (CNNIC) for IP addresses. Internet Corporation for Assigned Names and Numbers (ICANN) is the final organization responsible for IP address assignment. If the network to be built is an internal private network, users do not need to apply for IP addresses. However, IP addresses cannot be assigned at random. It is recommended to assign dedicated private network addresses.

The following table lists reserved and available addresses.

Class	Address Range	Status
Class A network	0.0.0.0 - 0.255.255.255	Reserved
	1.0.0.0 - 126.255.255.255	Available
	127.0.0.0 - 127.255.255.255	Reserved
Class B network	128.0.0.0 - 191.254.255.255	Available
	191.255.0.0 - 191.255.255.255	Reserved
Class C network	192.0.0.0 - 192.0.0.255	Reserved
	192.0.1.0 - 223.255.254.255	Available
	223.255.255.0 - 223.255.255.255	Reserved
Class D network	224.0.0.0 - 239.255.255.255	Multicast address
Class E network	240.0.0.0 - 255.255.255.254	Reserved
	255.255.255.255	Broadcast address

Three address ranges are dedicated to private networks. These addresses are not used in the Internet. If the networks to which these addresses are assigned need to be connected to the Internet, these IP addresses need to be converted into valid Internet addresses. The following table lists private address ranges. Private network addresses are defined in RFC 1918.

Class	Address Range	Status
Class A network	10.0.0.0 - 10.255.255.255	1 class A network
Class B network	172.16.0.0 - 172.31.255.255	16 class B networks
Class C network	192.168.0.0 - 192.168.255.255	256 class C networks

For assignment of IP addresses, TCP/UDP ports, and other codes, refer to RFC 1166.

Subnet Mask

A subnet mask is also a 32-bit value. The bits that identify the IP address are the network address. In a subnet mask, the IP address bits corresponding to the bits whose values are 1s are the network address, and the IP address bits corresponding to the bits whose values are 0s are the host address. For example, for class A networks, the subnet mask is 255.0.0.0. By using network masks, you can divide a network into several subnets. Subnetting means to use some bits of the host address as the network address, thus decreasing the host capacity, and increasing the number of networks. In this case, network masks are called subnet masks.

Broadcast Packet

Broadcast packets refer to the packets destined for all hosts on a physical network. Devices support two types of broadcast packets: (1) directed broadcast, which indicates that all hosts on the specified network are packet receivers and the host bits of a destination address are all 1s; (2) limited broadcast, which indicates that all hosts on all networks are packet receivers and the 32 bits of a destination address are all 1s.

ICMP Packet

Internet Control Message Protocol (ICMP) is a sub-protocol in the TCP/IP suite for transmitting control messages between IP hosts and network devices. It is mainly used to notify corresponding devices when the network performance becomes abnormal.

TTL

Time To Live (TTL) refers to the number of network segments where packets are allowed to pass before the packets are discarded. The TTL is a value in an IP packet. It informs the network whether packets should be discarded as the packets stay on the network for a long time.

Features

Feature	Description
IP Address	The IP protocol can run on an interface only after the interface is configured with an IP address.
Broadcast Packet Processing	Broadcast addresses are configured and broadcast packets are forwarded and processed.
Sending ICMP Packets	ICMP packets are sent and received.
Limiting Transmission Rate of ICMP Error Packets	This function prevents Denial of Service (DoS) attacks.
IP MTU	Maximum Transmission Unit (MTU) of IP packets on an interface is configured.
IP TTL	The TTL of unicast packets and broadcast packets is configured.
IP Routed Port Protection	The port filters the packets from the source port and forwards them through the same port.
IP Source Route	Source routes are checked.
IP Address Pool	The function assigns an IP address to the peer end through PPP negotiation.

1.3.1 IP Address

IP addresses are obtained on an interface in the following ways:

1. Manually configuring IP addresses
2. Obtaining IP addresses through DHCP
3. Obtaining IP addresses through PPP negotiation
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

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

- A network does not have enough host addresses. For example, a LAN now needs one class C network to allocate 254 addresses. However, when the number of hosts exceeds 254, one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on L2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on IP layer. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, you can connect the isolated subnets by creating a subnet of the isolated network and configuring a secondary address. One subnet cannot be configured on two or more interfaces of a device.

Obtaining an IP Addresses through PPP Negotiation

This command is supported on point-to-point interfaces only.

Through this configuration, a point-to-point interface accepts the IP address assigned by the peer end through PPP negotiation.

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.

Obtaining an IP Address through PPP Negotiation

- By default, the interface cannot obtain an IP address through PPP negotiation.
- The **ip address negotiate** command is used to configure IP address negotiation on a point-to-point interface.

Borrowing an IP Address from Other Interfaces

- By default, an interface is not configured with an IP address.
- The **ip unnumbered** command can be used to borrow IP addresses from other interfaces.

1.3.2 Broadcast Packet Processing

Working Principle

Broadcast is divided into two types. One is limited broadcast, and the IP address is 255.255.255.255. Because the broadcast is prohibited by routers, the broadcast is called local network broadcast. The other is directed broadcast. All host bits are 1s, for example, 192.168.1.255/24. The broadcast packets with these IP addresses can be forwarded.

If IP network devices forward limited broadcast packets (destination IP address is 255.255.255.255), the network may be overloaded, which severely affects network performance. This circumstance is called broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. L2 network devices such as bridges and switches forward and spread broadcast storms.

The best way to avoid broadcast storm is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast rather than limited broadcast to spread data.

For details about broadcast storms, see RFC 919 and RFC 922.

Directed broadcast packets refer to the broadcast packets destined for a subnet. For example, packets whose destination address is 172.16.16.255 are called directed broadcast packets. However, the node that generates the packets is not a member of the destination subnet.

After receiving directed broadcast packets, the devices not directly connected to the destination subnet forward the packets. After directed broadcast packets reach the devices directly connected to the subnet, the devices convert directed broadcast packets to limited broadcast packets (destination IP address is 255.255.255.255) and broadcast the packets to all hosts on the destination subnet at the link layer.

Related Configuration

Configuring an IP Broadcast Address

- By default, the IP broadcast address of an interface is 255.255.255.255.
- To define broadcast packets of other addresses, run the **ip broadcast-address** command on the interface.

Forwarding Directed Broadcast Packets

- By default, directed broadcast packets cannot be forwarded.
- On the specified interface, you can run the **ip directed-broadcast** command to enable directed broadcast packets forwarding. In this way, the interface can forward directed broadcast packets to networks that are directly connected. Broadcast packets can be transmitted within the destination subnet without affecting forwarding of other directed broadcast packets.
- On an interface, you can define an Access Control List (ACL) to transmit certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.3.3 Sending ICMP Packets

Working Principle

ICMP Protocol Unreachable Message

A device receives non-broadcast packets destined for itself, and he packets contain the IP protocol that cannot be processed by the device. The device sends an ICMP protocol unreachable message to the source host. Besides, if the device does not know a route to forward packets, it also sends an ICMP host unreachable message.

ICMP Redirection Message

Sometimes, a route may be less than optimal, which makes a device send packets from the interface that receives packets. If a device sends packets from an interface on which it receives the packets, the device sends an ICMP redirection message to the source, informing the source that the gateway is another device on the same subnet. In this way, the source sends subsequent packets according to the optimal path.

ICMP Mask Response Message

Sometimes, a network device sends an ICMP mask request message to obtain the mask of a subnet. The network device that receives the ICMP mask request message sends a mask response message.

Related Configuration

Enabling ICMP Protocol Unreachable Message

- By default, the ICMP Protocol unreachable message function is enabled on an interface.
- You can run the [**no**] **ip unreachables** command to disable or enable the function.

Enabling ICMP Redirection Message

- By default, the ICMP redirection message function is enabled on an interface.
- You can run the [**no**] **ip redirects** command to disable or enable the function.

Enabling ICMP Mask Response Message

- By default, the ICMP mask response message function is enabled on an interface.
- You can run the [**no**] **ip mask-reply** command to disable or enable the function.

Enabling Notifications of Expired TTL

- By default, notifications of expired TTL are enabled.
- You can run the **[no] ip ttl-expires enable** command to enable or disable the function.

Enabling Returning of Timestamp Reply

- By default, a Timestamp Reply is not sent.
- You can run the **[no] ip icmp timestamp** command to enable or disable the function.

1.3.4 Limiting Transmission Rate of ICMP Error Packets

Working Principle

This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm.

If an IP packet needs to be fragmented but the Don't Fragment (DF) bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively.

Related Configuration

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by DF Bit in the IP Header

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval DF** command can be used to configure the transmission rate.

Configuring the Transmission Rate of Other ICMP Error Packets

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval** command can be used to configure the transmission rate.

1.3.5 IP MTU

Working Principle

If an IP packet exceeds the IP MTU size, the RGOS software splits the packet. For all devices in the same physical network segment, the IP MTU of interconnected interfaces must be the same. You can adjust the link MTU of interfaces on devices. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

Related Configuration

↘ Setting the IP MTU

- By default, the IP MTU of an interface is 1500.
- The **ip mtu** command can be used to set the IP packet MTU.

1.3.6 IP TTL

Working Principle

An IP packet is transmitted from the source address to the destination address through routers. After a TTL value is set, the TTL value decreases by 1 every time when the IP packet passes a router. When the TTL value drops to zero, the router discards the packet. This prevents infinite transmission of useless packets and waste of bandwidth.

Related Configuration

↘ Setting the IP TTL

- By default, the IP TTL of an interface is 64.
- The **ip ttl** command can be used to set the IP TTL of an interface.

1.3.7 IP Routed Port Protection

Working Principle

The port filters the packets from the source port and forwards them through the same port.

Related Configuration

↘ Configuring IP Routed Port Protection

- By default, the IP routed port protection function is disabled.
- Run the **ip redirect-drop** command to enable IP routed port protection.

1.3.8 IP Source Route

Working Principle

Devices 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.

1.3.9 IP Address Pool

Working Principle

A point-to-point interface can assign an IP address to the peer end through PPP negotiation. During PPP negotiation, the server checks authentication information of the client. If the client passes the authentication, the server assigns an IP address to the client (if the client is configured with an IP address and the IP address meets requirements of the server, the server approves the IP address of the client). The IP address of the peer end can be directly specified or assigned from the address pool.

Related Configuration

↘ Enabling the Address Pool Function

- By default, the address pool function is enabled.
- The **ip address-pool local** command can be used to enable or disable the function.

↘ Creating an Address Pool

- By default, no IP address pool is configured.
- The **ip local pool** command can be used to create or delete an address pool.

↘ Assigning an IP Address to the Peer End through PPP Negotiation

- By default, an interface does not assign an IP address to the peer end.
- The **peer default ip address** command can be used to assign an IP address to the peer end.

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.
	ip address negotiate	Obtains the IP address of an interface through PPP negotiation.
	ip unnumbered	Borrows an IP address from another interface.
Configuring Broadcast Forwarding	(Optional) It is used to set an IP broadcast address and enable directed broadcast forwarding.	
	ip broadcast-address	Configures an IP broadcast address.
	ip directed-broadcast	Enables directed broadcast forwarding.
Configuring ICMP Forwarding	(Optional) It is used to enable ICMP packet forwarding.	
	ip unreachables	Enables ICMP unreachable messages and host unreachable messages.
	ip redirects	Enables ICMP redirection messages.
	ip mask-reply	Enables ICMP mask response messages.
	ip ttl-expires enable	Enables notifications of expired TTL.
	ip icmp timestamp	Enables returning of Timestap Reply.
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 MTU	(Optional) It is used to configure the IP MTU on an interface.	
	ip mtu	Sets the MTU value.
Setting the IP TTL	(Optional) It is used to configure the TTL of unicast packets and broadcast packets.	
	ip ttl	Sets the TTL value.
Configuring IP Routed Port Protection	(Optional) It is applicable to a Layer 3 routed port only.	
	ip redirect-drop	
Configuring an IP Source Route	(Optional) It is used to check the source routes.	
	ip source-route	Enables the IP source route function.

Configuration	Description and Command	
Configuring an IP Address Pool	(Optional) It is used to configure an IP address pool.	
	ip address-pool local	Enables the IP address pool function
	ip local pool	Creates an IP address pool
	peer default ip address	Assigns an IP address to the peer end through PPP negotiation

1.4.1 Configuring the IP Addresses of an Interface

Configuration Effect

Configure the IP address of an interface for communication.

Notes

- N/A

Configuration Steps

Configuring the IP Address of an Interface

- Mandatory
- Perform the configuration in L3 interface configuration mode.

Obtaining the IP Address of an Interface through PPP Negotiation

- If a point-to-point interface is not configured with an IP address, obtain an IP address through PPP negotiation.
- Perform the configuration in L3 interface configuration mode.

Borrowing an IP Address from Another Interface

- Optional
- If a point-to-point interface is not configured with an IP address, borrow an IP address from another interface.
- Perform the configuration in L3 interface configuration mode.

Verification

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

Related Commands

Manually Configuring the IP Address of an Interface

Command	**ip address** *ip-address network-mask* [**secondary**]
Parameter Description	*ip-address*: 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal and groups are separated by a full stop (.). *network-mask*: 32-bit network mask. Value 1 indicates the mask bit and 0 indicates the host bit. Every

	8 bits form one group. The network mask is expressed in decimal and groups are separated by a full stop (.). **secondary**: Secondary IP address.
Command Mode	Interface configuration mode
Usage Guide	N/A

↘ Obtaining an IP Address of an Interface through PPP Negotiation

Command	**ip address negotiate**
Parameter Description	N/A
Command Mode	Dialer Interface configuration mode
Usage Guide	Only point-to-point interfaces support obtaining IP addresses through PPP negotiation. After the **ip address negotiate** command is run on an interface, run the **peer default ip address** command at the peer end.

↘ Borrowing an IP Addresses from Another Interface

Command	**ip unnumbered** *interface-type interface-number*
Parameter Description	*interface-type*: Interface type. *interface-number*: Interface ID.
Command Mode	Interface configuration mode
Usage Guide	An unnumbered interface indicates that the interface is enabled with the IP protocol without an IP address assigned. An unnumbered interface needs to be associated with an interface configured with an IP address. For an IP packet generated on an unnumbered interface, the source IP address of the packet is the IP address of the associated interface. In addition, the routing protocol process decides whether to send a route update packet to the unnumbered interface according to its associated IP address. If you want to use an unnumbered interface, pay attention to the following limitations: An Ethernet interface cannot be set to an unnumbered interface. When a serial interface encapsulates SLIP, HDLC, PPP, LAPB, and Frame-Relay, the serial interface can be set to an unnumbered interface. During Frame -Relay encapsulation, however, only a point-to-point interface can be configured as an unnumbered interface. AnX.25 interface cannot be configured as an unnumbered interface. The **ping** command cannot be used to check whether an unnumbered interface is working properly because an unnumbered interface is not configured with an IP address. However, you can monitor the status of an unnumbered interface remotely through SNMP. A device cannot be cold started through an unnumbered interface.

Configuration Example

↘ Configuring an IP Address for an Interface

Configuratio	Configure IP address 192.168.23.110 255.255.255.0 on interface GigabitEthernet 0/1.

n Steps	
	Hostname#configure terminal Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# no switchport Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.23.110 255.255.255.0
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Hostname# show ip interface gigabitethernet 0/1 GigabitEthernet 0/1 IP interface state is: UP IP interface type is: BROADCAST IP interface MTU is: 1500 IP address is: 192.168.23.110/24 (primary)

↘ Obtaining the IP Address of an Interface through PPP Negotiation

Configuration Steps	Obtain the IP address of an interface through PPP negotiation.
	Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)#ip address negotiate
Verification	Run the **show run** command on the AC to display the configuration.
	Hostname#show run interface virtual-ppp 1 Building configuration... Current configuration: 48 bytes interface Virtual-ppp 1 ip address negotiate

1.4.2 Configuring Broadcast Forwarding

Configuration Effect

Set the broadcast address of an interface to 0.0.0.0 and enable directed broadcast forwarding.

Notes

N/A

Configuration Steps

Configuring an IP Broadcast Address

- (Optional) Some old hosts may identify broadcast address 0.0.0.0 only. In this case, set the broadcast address of the target interface to 0.0.0.0.
- Perform the configuration in L3 interface configuration mode.

Enabling Directed Broadcast Forwarding

- (Optional) If you want to enable a host to send broadcast packets to all hosts in a domain that it is not in, enable directed broadcast forwarding.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show running-config interface** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Broadcast Address

Command	**ip broadcast-address** *ip-address*
Parameter Description	*ip-address*: Broadcast address of an IP network.
Command Mode	Interface configuration mode
Usage Guide	Generally, the destination address of IP broadcast packets is all 1s, which is expressed as 255.255.255.255. The 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.

Allowing Forwarding of Directed Broadcast Packets

Command	**ip directed-broadcast** [*access-list-number*]
Parameter Description	*access-list-number*: Access list number, ranging from 1 to 199 and from1300 to 2699. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.
Command Mode	Interface configuration mode
Usage Guide	If the **no ip directed-broadcast** command is run on an interface, the RGOS software will discard directed broadcast packets received from the network that is directly connected.

Configuration Example

Configuration Steps	On interface GigabitEthernet 0/1, set the destination address of IP broadcast packets to 0.0.0.0 and enable directed broadcast forwarding. Hostname#configure terminal Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# no switchport Hostname(config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0 Hostname(config-if-GigabitEthernet 0/1)#ip directed-broadcast
Verification	Run the **show ip interface** command to check whether the configuration takes effect. Hostname#show running-config interface gigabitEthernet 0/1 ip directed-broadcast ip broadcast-address 0.0.0.0

1.4.3 Configuring ICMP Forwarding

Configuration Effect

Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on an interface.

Notes

N/A

Configuration Steps

Enabling ICMP Unreachable Messages

- By default, ICMP unreachable messages are enabled.
- Optional)The **no ip unreachables** command can be used to disable ICMP unreachable messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Redirection Messages

- By default, ICMP redirection messages are enabled.
- Optional)The **no ip redirects** command can be used to disable ICMP redirection messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Mask Response Messages

- By default, ICMP mask response messages are enabled.
- Optional)The **no ip mask-reply** command can be used to disable ICMP mask response messages.
- Perform the configuration in L3 interface configuration mode.

Enabling Notifications of Expired TTL

- By default, notifications of expired TTL are enabled.

- (Optional)The **[no]ip ttl-expires enable** command can be used to enable or disable the function.
- Perform the configuration in global configuration mode.

Enabling Returning of Timestamp Reply

- By default, returning of Timestamp Reply is enabled.
- (Optional)The **[no] ip icmp timestamp c**ommand can be used to enable or disable the function.
- Perform the configuration in global configuration mode.

Verification

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

Run the **show running-config** command to check whether notifications of expired TTL are disabled.

Run the **show running-config** command to check whether returning of Timestamp Reply is enabled.

Related Commands

Enabling ICMP Unreachable Messages

Command	**ip unreachables**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Redirection Messages

Command	**ip redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Mask Response Messages

Command	**ip mask-reply**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Disabling Notifications of Expired TTL

Command	**no ip ttl-expires enable**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Disabling Returning of Timestamp Reply

Command	**no ip icmp timestamp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on interface GigabitEthernet 0/1.
	Hostname#configure terminal Hostname(config)# no ip ttl-expires enable Hostname(config)# no ip icmp timestamp Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# no switchport Hostname(config-if-GigabitEthernet 0/1)# ip unreachables Hostname(config-if-GigabitEthernet 0/1)# ip redirects Hostname(config-if-GigabitEthernet 0/1)# ip mask-reply
Verification	Run the **show ip interface** command to check whether the configuration takes effect.

	Hostname#show running-config | include ip ttl-expires enable no ip ttl-expires enable Hostname#show running-config | include ip icmp timestamp no ip icmp timestamp Hostname#show ip interface gigabitethernet 0/1 GigabitEthernet 0/1 ICMP mask reply is: ON Send ICMP redirect is: ON Send ICMP unreachabled is: ON

1.4.4 Configuring the Transmission Rate of ICMP Error Packets

Configuration Effect

Configure the transmission rate of ICMP error packets.

Notes

N/A

Configuration Steps

↘ **Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header**

- Optional
- Perform the configuration in global configuration mode.

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

- Optional
- Perform the configuration in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ **Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header**

Command	**ip icmp error-interval DF** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is from 0 to 2,147,483,647 and the default value is 100 milliseconds. When the value is 0, the transmission rate of ICMP error packets is

	not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. If an IP packet needs to be fragmented but the DF bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10milliseconds.

↘ Configuring the Transmission Rate of Other ICMP Error Packets

Command	**ip icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is 0to 2,147,483,647, and the default value is **100** (ms). When the value is **0**, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is 1to 200 and the default value is **10**.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds.

Configuration Example

Configuration Steps	Set the transmission rate of ICMP destination unreachable packets triggered the DF bit in IP header to 100 packets per second and the transmission rate of other ICMP error packets to 10 packets per second.

	Hostname(config)# ip icmp error-interval DF 1000 100 Hostname(config)# ip icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Hostname#show running-config | include ip icmp error-interval ip icmp error-interval 1000 10 ip icmp error-interval DF 1000 100

1.4.5 Setting the IP MTU

Configuration Effect

Adjust the IP packet MTU.

Notes

N/A

Configuration Steps

- (Optional) When the IP MTU of interconnected interfaces is different on devices in the same physical network segment, set the IP MTU to the same value.
- Perform the configuration in L3 interface configuration mode.

Verification

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

Related Commands

↘ Setting the IP MTU

Command	**ip mtu** *bytes*
Parameter Description	*bytes*: IP packet MTU. The value range is from 68 to 1,500 bytes.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the IP MTU of interface GigabitEthernet 0/1 to 512 bytes.

	Hostname#configure terminal Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# no switchport Hostname(config-if-GigabitEthernet 0/1)#ip mtu 512
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Hostname# show ip interface gigabitEthernet 0/1 IP interface MTU is: 512

1.4.6 Setting the IP TTL

Configuration Effect

Modify the IP TTL value of an interface.

Notes

N/A

Configuration Steps

- Optional
- Perform the configuration in L3 interface configuration mode.

Verification

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

Related Commands

↘ Setting the IP TTL

Command	**ip ttl** *value*
Parameter Description	*value*: TTL value. The value range is from 0 to 255.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	• Set the TTL of unicast packets to 100.
	Hostname#configure terminal Hostname(config)#ip ttl 100

Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Hostname#show running-config ip ttl 100

1.4.7 Configuring IP Routed Port Protection

Configuration Effect

Enable IP routed port protection.

Notes

-

Configuration Steps

- Optional
- Applicable to a Layer 3 routed port only.

Verification

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

Related Commands

↘ **Configuring IP Routed Port Protection**

Command	ip redirect-drop
Parameter Description	N/A
Command Mode	Interface configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	• Enable routed port protection on GigabitEthernet 0/1.
	Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip redirect-drop
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Hostname#show running-config ip redirect-drop

1.4.8 Configuring an IP Source Route

Configuration Effect

Enable or disable the IP source route function.

Notes

N/A

Configuration Steps

- By default, the IP source route function is enabled.
- Optional) The **no ip source-route** command can be used to disable the IP source route function.

Verification

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

Related Commands

↘ **Configuring an IP Source Route**

Command	**ip source-route**
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	● Disable the IP source route function.
	Hostname#configure terminal Hostname(config)#no ip source-route
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Hostname#show running-config no ip source-route

1.4.9 Configuring an IP Address Pool

Configuration Effect

Assign an IP address to a client through PPP negotiation.

Notes

N/A

Configuration Steps

Enabling the IP Address Pool Function

- Optional
- Perform the configuration in global configuration mode.

Creating an IP Address Pool

- Optional
- An IP address pool can be created only after the IP address pool function is enabled. After the IP address pool function is disabled, the created address pool is automatically deleted.
- Perform the configuration in global configuration mode.

Assigning an IP Address to the Peer End through PPP Negotiation

- Optional
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Enabling the IP Address Pool Function

Command	**ip address-pool local**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the IP address pool function is enabled. You can configure an IP address pool to assign an IP address to the peer end through PPP negotiation. To disable the IP address pool function, run the **no ip address-pool local** command. All IP address pools configured previously will be deleted.

Creating an IP Address Pool

Command	**ip local pool** *pool-name low-ip-address* [*high-ip-address*]
Parameter Description	*pool-name*: Name of a local IP address pool. **default** indicates the default address pool name. *low-ip-address*: Smallest IP address in an IP address pool. *high-ip-address*: Optional)Largest IP address in an IP address pool. If the largest IP address is not specified, the IP address pool contains only one IP address, that is, *low-ip-address*.
Command Mode	Global configuration mode
Usage Guide	The command is used to create one or more IP address pools to assign IP addresses to peer ends through PPP negotiation.

Assigning an IP Address to the Peer End through PPP Negotiation

Command	**peer default ip address** { *ip-address* | **pool** [*pool-name*] }
Parameter Description	*ip-address*: IP address assigned to the peer end. *pool-name*: (Optional) Specifies the address pool that assigns IP addresses. If this parameter is not set, IP addresses are assigned from the default address pool.
Command Mode	Interface configuration mode
Usage Guide	If the peer end is not configured with an IP address while the local device is configured with an IP address, you can enable the local device to assign an IP address to the peer end. Run the **ip address negotiate** command on the peer end and the **peer default ip address** command on the local device so that the peer end can accept the IP address assigned through PPP negotiation. The **peer default ip address** command can be configured on only PPP or SLIP interfaces. The **peer default ip address pool** command is used to assign an IP address to the peer end from an IP address pool. The IP address pool is configured through the **ip local pool** command. The **peer default ip address** *ip-address* command is used to specify an IP address for the peer end. The command cannot be run on virtual template interfaces or asynchronous interfaces.

Configuration Example

Configuration Steps	● Assign an IP address from address pool “quark” to the peer end on interface “dialer1”.
	Hostname#configure terminal Hostname(config)# ip address-pool local Hostname(config)# ip local pool quark 172.16.23.2 172.16.23.255 Hostname(config)# interface dialer 1 Hostname(config-if-dialer 1)#peer default ip address pool quark
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Hostname#show running-config ip local pool quark 172.16.23.2 172.16.23.255 ! interface dialer 1 peer default ip address pool quark

1.5 Monitoring

Displaying

Description	Command
Displays the IP address of an interface.	**show ip interface** [*interface-type interface-number* | **brief**]

Displays IP packet statistics.	**show ip packet statistics** [**total** | *interface-name*]
Displays the statistics of IP packet queues.	**show ip packet queue**
Displays IPv4 raw sockets	**show ip raw-socket** [num]
Displays all IPv4 sockets.	**show ip sockets**
Displays IPv4 UDP sockets.	**show ip udp** [**local-port** num]
Displays statistics on IPv4 UDP sockets.	**show ip udp statistics**

1 Configuring NAT

1.1 Overview

Network Address Translation (NAT) is a process of translating the IP address in the header of an IP data packet into another IP address. In practice, NAT enables private networks that use unregistered IP addresses to access public networks. This way of using a small number of public IP addresses to represent substantial private IP addresses implements IP address conservation.

Protocols and Standards

- RFC 1631: The IP Network Address Translator (NAT)
- RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations
- RFC 2391: Load Sharing using IP Network Address Translation (LSNAT)
- RFC 4008: Definitions of Managed Objects for Network Address Translators (NAT)

1.2 Applications

Application	Description
Intranet Users' Access to the Internet	NAT allows an intranet to communicate with the Internet by translating an inside private IP address into a globally unique IP address.
External Users' Access to an Intranet Server	NAT allows external networks to access internal devices by mapping one or more internal hosts to a network server.
Source/Destination Address Translation for Internal Users	When two private networks to interconnect with each other are configured with the same IP address or the same global IP address is allocated to both a private network and a public network, the two network hosts with the same IP address cannot communicate. NAT allows overlapping networks to communicate.
Intranet Server Load Balancing	When the TCP traffic load of an intranet host is excessively heavy, multiple hosts are deployed for TCP service load balancing. In this case, NAT may be used to attain this objective.

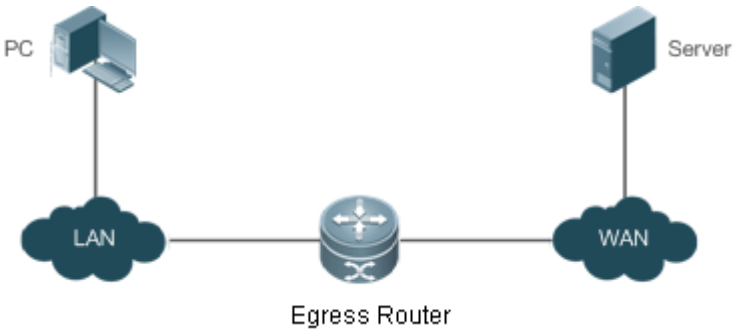
1.2.1 Intranet Users' Access to the Internet

Scenario

A PC is located in an intranet while a server is located in an extranet, as shown in Figure 11-1. In view of IP address depletion, only one or a few public IP addresses are allocated to the entire campus network. An egress router

belongs to the intranet, and connects to the extranet. The basic NAT function is required on the egress device to allow the intranet PC to access the extranet server.

Figure 1-1



The egress device connects both the intranet and the extranet.

Corresponding Protocols

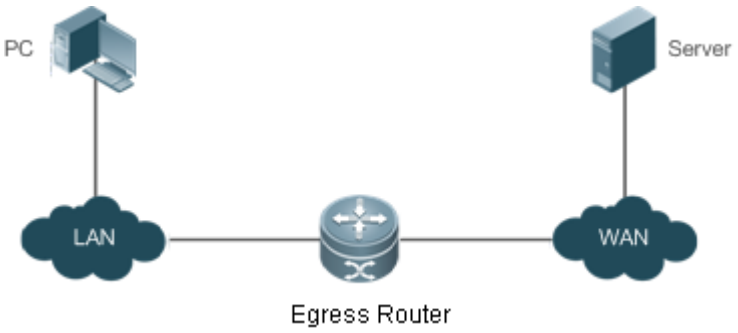
- Configure an inside interface and an outside interface for NAT.
- Configure static inside source address translation on the egress router.

1.2.2 External Users' Access to an Intranet Server

Scenario

A PC is located in an extranet while a server (such as a Web server) is located in an intranet, as shown in Figure 11-2. In view of IP address depletion, only one public IP address is allocated to the entire campus network. An egress device belongs to the intranet, and connects to the extranet. The Network Address and Port Translation (NAPT) function is required on the egress device to enable the PC to access the intranet server; that is, port mapping applies to the Web service port.

Figure 1-2



The egress device connects both the intranet and the extranet.
The server is deployed in the intranet.

Corresponding Protocols

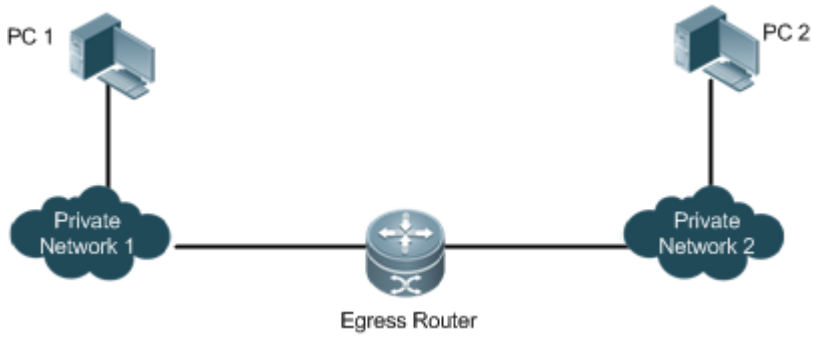
- Configure an inside interface and an outside interface for NAT.
- Configure server port address translation rules on the egress router.

1.2.3 Source/Destination Address Translation for Internal Users

Scenario

PC 1 is located in private network 1 while PC 2 is located in private network 2, as shown in Figure 11-3. Because the two private networks are separately managed, address overlapping occurs in their IP network segments. For example, the IP addresses of PC 1 and PC 2 are configured in the same network segment 192.168.1.0/24. An egress device is located between private networks 1 and 2. The NAT function needs to be enabled on the egress device, so that PC 1 and PC 2 can access each other.

Figure 1-3



The egress device connects both private networks.

Corresponding Protocols

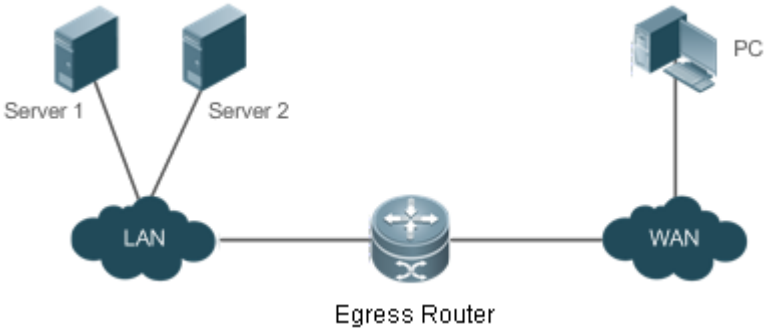
- Configure an inside interface and an outside interface for NAT.
- Configure dynamic translation of the inside source address on the egress router.
- Configure dynamic translation of the outside source address on the egress router.

1.2.4 Intranet Server Load Balancing

Scenario

Server 1 and Server 2 are located in an intranet, and form a cluster, as shown in Figure 11-4. A PC is located in an extranet. In view of IP address depletion, only one public IP address is allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The egress device needs to distribute the server access traffic of the external user to the two servers; therefore, the NAT load balancing function needs to be enabled on the egress device.

Figure 1-4



The egress device connects both the intranet and the extranet.
The servers are deployed in the intranet.

Corresponding Protocols

- Configure an inside interface and an outside interface for NAT.
- Configure TCP load balancing using NAT on the egress router.

1.3 Features

Basic Concepts

Private Address and Public Address

A private address is the IP address of an intranet or an intranet host, whereas a public address is an IP address globally unique on the Internet. The Internet Assigned Numbers Authority (IANA) has stipulated the following IP addresses for use on private networks, which cannot be allocated for use on the Internet but can be used inside any institution or corporation.

Class A private addresses: 10.0.0.0 to 10.255.255.255

Class B private addresses: 172.16.0.0 to 172.31.255.255

Class C private addresses: 192.168.0.0 to 192.168.255.255

NAT was initially designed to enable a private network to access a public network. Later it was extended to implement address translation for mutual access between any two networks. In this document, the two networks are called an intranet and an extranet. In general, a private network is an intranet, and a public network is an extranet.

Static NAT

Static NAT allows one-to-one permanent mappings between inside local addresses and inside global addresses. Static NAT is important when an extranet needs to access internal hosts via a fixed global routable address.

Dynamic NAT

Dynamic NAT establishes temporary mapping relationships between inside local addresses and inside global addresses. The temporary mapping relationships will be removed when unused in a certain period of time.

Dynamic NAT can be configured in the following case: An intranet accesses extranet services only but does not provide services, and the number of intranet hosts is greater than the number of global IP addresses.

Overview

Feature	Description
Basic NAT	This feature translates inside private addresses into globally unique addresses, so that the intranet and the public network can communicate with each other.
NAPT	This feature maps multiple inside local addresses to one inside global address, so as to resolve the problem of IP address depletion.
Overlapping NAT	This feature enables overlapping networks to communicate.
TCP Load Balancing	This feature resolves the problem of TCP traffic overload.
Constructing a Local Server	This feature enables extranet to access the local server.
ALG	NAT changes only the header of an IP packet but not the payload of a specific application protocol. Therefore, the Application Level Gateway (ALG) is introduced to support application layer protocols.

1.3.1 Basic NAT

NAT is required for an intranet to communicate with an extranet by translating an inside private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection and interworking.

Working Principle

An IP packet sent by an intranet host (192.168.1.2) to an extranet server (8.8.8.8) reaches an NAT device.

The NAT device checks the content of the IP packet, and finds that the IP packet is destined to an extranet. Therefore, the NAT device translates the private IP address 192.168.1.2 in the source IP address field of the IP packet into a public IP address 30.1.1.1 routable on the Internet, sends the IP packet to the extranet server, and at the same time records the mapping in its own NAT table.

The extranet server returns a response packet (in which the initial destination IP address is 30.1.1.1) to the intranet user. When the response packet reaches the NAT device, the NAT device checks the content of the response packet, looks up the mapping record in the NAT table, and replaces the initial destination IP address with the inside private IP address 192.168.1.2.

The above NAT process is transparent to terminals, such as the host and the server shown in the preceding figures. In the point of view of the extranet server, the IP address of the intranet host is 30.1.1.1 and the extranet server itself does not know the existence of the IP address 192.168.1.2 at all. Therefore, NAT "hides" the private network of an enterprise.

Basic NAT includes static NAT and dynamic NAT.

Related Configuration

Configuring NAT Interfaces

- A routed port is not an NAT interface by default.
- For a routing interface, run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces. For a non-routing interface, run the **no switchport** command and then the **ip nat inside/outside** command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Static NAT

- Static NAT is not configured by default.
- Use the **ip nat inside source static** *local-ip global-ip* [**permit-inside**] [**netmask** *mask* | **match** *interface-type interface-number*] command to configure static one-to-one NAT mapping.

Configuring Dynamic NAT

- Dynamic NAT is not configured by default.
- Use the **ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**] command to configure dynamic NAT mapping.

1.3.2 NAPT

In general, traditional NAT is one-to-one address mapping, which, however, cannot meet the requirements of all hosts in intranets to communicate with extranets. For example, when the intranet is in short of global IP addresses or even does not apply for global IP addresses but has only one global IP address to connect to an Internet Service Provider (ISP) while a large number of hosts in the intranet need to access the Internet, NAPT is required in this scenario.

Multiple inside local addresses can map to one inside global address using NAPT.

When NAPT mappings to a large number of public IP addresses are configured and NAPT is deployed on the egress gateway in VRRP routing redundant scenarios, association between the VRRP groups and extranet interface link status and protocol status needs to be used if extranet attacks exist. In addition, the advertisement configuration times need to be adjusted using VRRP to reduce the switchover frequency between the active and standby VRRP groups. To ensure that the NAT device can send free ARP packets from local host addresses and respond to ARP requests correctly during a switchover between the active and standby VRRP groups, you should associate the NAT device with a VRRP group and restrict the rate to send free ARP packets.

Working Principle

NAPT, also known as multiple-to-one address translation, allows multiple inside addresses to map to one public address. NAPT maps both IP addresses and port numbers; that is, the source addresses of data packets from different inside addresses can map to the same public address, but their port numbers are translated into

different port numbers of the public address so that the same address can still be shared. NAPT is translation between "private IP address + Port number" and "Public IP address + Port number".

Static NAPT

In general, static NAPT is used to map the specified port on a specified host in an intranet to the specified port of a global address. In comparison, as mentioned previously, static NAT maps an internal host to a global address. Static NAPT is applicable to intranet hosts that provide the information service. Static NAPT provides a permanent one-to-one "IP address + Port" mapping relationship.

Dynamic NAPT

Dynamic NAPT is applicable to intranet hosts that only access extranet services but do not provide any information service. Dynamic NAPT provides a temporary one-to-one "IP address + Port" mapping relationship.

Related Configuration

Configuring NAT Interfaces

- A routed port is not an NAT interface by default.
- If the port is a routed port, run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces. If not, configure the port as a routed port and run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Static NAPT

- Static NAPT is not configured by default.
- Use the **ip nat inside source static** *local-ip global-ip* [**permit-inside**] command to configure static one-to-one NAPT mapping.

Configuring Dynamic NAPT

- Dynamic NAPT is not configured by default.
- Use the **ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**] command to configure dynamic NAPT mapping. For NAPT, generally only one IP address is defined in the address pool, and one IP address supports up to 64,512 times of NAT. If one IP address is not enough, multiple IP addresses can be defined in the address pool.

1.3.3 Overlapping NAT

When the same IP address is allocated to two private networks to interconnect with each other or the same global IP address is allocated to a private network and a public network, this situation is called address overlapping. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is in the local network. Overlapping NAT is especially designed to implement the communications between two networks with

the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address in the intranet, and vice versa.

Working Principle

For mutual access between an intranet and an extranet with the same IP address, NAT needs to translate the inside address into a unique outside address. In addition, NAT needs to translate the outside address that overlaps with the inside address into another unique inside address.

Related Configuration

Configuring NAT Interfaces

- A routed port is not a NAT interface by default.
- If the port is a routed port, run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces. If not, configure the port as a routed port and run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Inside Source Address Translation

- Inside source address translation is not configured by default.
- Static/dynamic basic NAT or static/dynamic NAPT can be used for inside source address translation. For details, see the "Basic NAT" and "NAPT" sections.

Configuring Static Translation of Outside Source Address

- Static translation of outside source address is not configured by default.
- Use the **ip nat outside source static** *global-ip local-ip* command to configure static translation of outside source address.

Configuring Dynamic Translation of Outside Source Address

- Dynamic translation of outside source address is not configured by default.
- Use the **ip nat outside source list** *access-list-number* **pool** *pool-name* command to configure dynamic translation of outside source address.

Configuring an ACL

- No ACL is configured by default.
- Use the **ip access-list** { **extended | standard** } { *id* | *name* } command or the **access-list** command to configure an ACL.

Configuring a Static Route

- Mandatory configuration.

- Use the **ip route** *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent | track** *object-number*] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**] command to configure a static route, which is used to specify the network egress after inside destination address translation.

1.3.4 TCP Load Balancing

When the TCP traffic load of an intranet host is excessively heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to attain this objective.

Working Principle

Create a virtual host with NAT to provide the TCP service. The virtual host maps to multiple physical hosts. Then the virtual host polls and replaces destination addresses, so as to implement traffic load distribution.

Related Configuration

↘ Configuring NAT Interfaces

- A routed port is not an NAT interface by default.
- If the port is a routed port, run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces. If not, configure the port as a routed port and run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

↘ Configuring the Address Pool

- No address pool is configured by default.
- Use the **ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**] command to configure an IP address pool for NAT.

↘ ACL

- No ACL is configured by default.
- Use the **access-list** *access-list-number* **permit** *ip-address wildcard* command to configure a destination-based ACL. Note that the ACL must be configured as an extended ACL based on destination IP address matching.

↘ Configuring Inside Destination Address Translation

- Inside destination address translation is not configured by default.
- Use the **ip nat inside destination list** *access-list-number* **pool** *poo-namel* command to configure inside destination address translation. This configuration takes effect on TCP traffic only but not on other traffic, unless additional NAT configuration has been performed.

1.3.5 Constructing a Local Server

A user has deployed three servers (an FTP server, a Web server, and an Email server) in an intranet, and hopes that network hosts in a WAN can access the three servers while common users of the intranet can set the gateway as a device to provide Internet access.

Working Principle

Map one or more internal hosts to a network server, so that users on the WAN obtain corresponding services from the network server.

Related Configuration

↘ Configuring NAT Interfaces

- A routed port is not an NAT interface by default.
- If the port is a routed port, run the **ip nat** { inside | outside } command to specify a pair of NAT interfaces. If not, configure the port as a routed port and run the **ip nat** { inside | outside } command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

↘ Configuring Inside Address and Port Translation

- Inside address and port translation is not configured by default.
- Use the **ip nat inside source static** { **udp** | **tcp** } **local-ip port global-ip port** [**permit-inside**] command to translate specific inside addresses and ports, so that corresponding services are provided on dedicated ports. For example, TCP port 20 or 21 can be used to construct an FTP server, or TCP port 80 to construct a Web server.

1.3.6 ALG

Common NAT can translate the IP address and port in the header of a UDP or TCP packet, but is helpless before fields in application layer data payloads. In many application layer protocols such as multimedia protocols (H323 and the like), FTP, and SQLNET, the TCP/UDP payload carries address or port information. If such address or port information cannot be translated by NAT, problems may occur.

Working Principle

The ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process the IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing the correctness of application layer communications. All types of ALGs are enabled for NAT by default. Currently the protocols that support ALG include DNS, FTP, H323, PPTP, TFTP, RTSP, and SIP.

Related Configuration

Enabling or Disabling ALG

- By default, all ALGs are enabled.
- Use the **no ip nat translation dns** command to disable DNS ALG.
- Use the **no ip nat translation ftp** command to disable FTP ALG.
- Use the **no ip nat translation h323** command to disable H323 ALG.
- Use the **no ip nat translation pptp** command to disable PPTP ALG.
- Use the **no ip nat translation tftp** command to disable TFTP ALG.
- Use the **no ip nat translation rtsp** command to disable RTSP ALG.
- Run the **no ip nat translation sip** command to disable SIP ALG.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic NAT	⚠ Mandatory configuration. It is used to configure one-to-one NAT for internal PCs to connect to a WAN.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	⚠ Optional configuration. It is used to configure static NAT.	
	ip nat inside source static *local-ip global-ip* [**permit-inside**] [**netmask** *mask* | **match** interface]	Defines the static inside source address translation relationship.
	⚠ Optional configuration. It is used to configure dynamic NAT.	
	ip nat pool pool-name [start-ip end-ip] { **netmask** mask | **prefix-length** prefix-length } [**type rotary**] or **ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**] **address** *start-ip end-ip* [**match interface** *interface*]	Defines a global IP address pool. For NAT, generally multiple IP addresses are defined. The number of address pools to be defined shall depend on the number of intranet users.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.

	ip nat inside source list *access-list-number* { **interface** *interface-type interface-number* | **pool** *poo-namel* } [**overload**]	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration .
Configuring NAPT	⚠ Mandatory configuration. It is used to configure NAPT.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	⚠ Optional configuration. It is used to configure static NAPT.	
	ip nat inside source static { **UDP** *local-ip port* | **TCP** *local-ip port* } *global-ip port* [**permit-inside**]	Defines the static inside source address translation relationship.
	⚠ Optional configuration. It is used to configure dynamic NAPT.	
	ip nat pool *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]	Defines a global IP address pool. For NAPT, generally only one IP address is defined.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat inside source list *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring Overlapping NAT	⚠ Mandatory configuration. It is used to enable overlapping networks to communicate using NAT.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	ip nat inside source static *local-ip global-ip*	Configures inside source address translation.
	⚠ Optional configuration. It is used to configure static NAT.	
	ip nat outside source static *global-ip local-ip*	Configures static NAT.
	⚠ Optional configuration. It is used to configure dynamic NAT.	

	ip nat pool *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]	Defines a global IP address pool.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat outside source list *access-list-number* **pool** *pool-name*	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring TCP Load Balancing	⚠ Mandatory configuration. It is used to configure destination address polling and translation.	
	ip nat inside	Marks the interface as connected to inside.
	ip nat outside	Marks the interface as connected to outside.
	ip nat pool *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]	Defines an IP address pool, which includes all physical host addresses.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, which matches the virtual host address only. ⚠ Ensure that the ACL is an extended ACL based on destination IP address matching.
	ip nat inside destination list *access-list-number* **pool** *pool-name*	Defines the dynamic inside destination address translation relationship.
Configuring ALG	⚠ Optional configuration. It is used to configure ALG for relevant protocols.	
	ip nat translation { **dns** [**ttl** *ttl_time*] | **ftp** [**port** *port_num*] | **h323** | **pptp** | **rtsp** | **sip** | **tftp** [**port** *port_num*] }	Defines ALG for relevant protocols.
Configuring Special NAT Applications	⚠ Optional configuration. It is used to configure special NAT applications.	
	ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-address* | **src-change** *ip-address* }	Defines rules for special NAT applications.
Configuring the Interval at Which NAT Sends Gratuitous ARP Packets	⚠ Optional configuration. It is used to configure the interval at which gratuitous ARP packets are sent from the local address of NAT.	
	ip nat keepalive [*keealive_out*]	Defines the interval at which gratuitous ARP packets are sent from the local address of NAT.

1.4.1 Configuring Basic NAT

Networking Requirements

NAT configuration is required for an intranet to communicate with an extranet by translating an inside private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection and interworking.

Notes

- At least one inside interface and one outside interface need to be configured for basic NAT.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

↘ Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

↘ Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

↘ Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Verification

N/A

Commands

↘ Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
Command	Interface configuration mode

Mode	
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the device.

Configuring Static NAT

Command	**ip nat inside source static** *local-ip global- ip* [**permit-inside**] [**netmask** *mask* | **match** *interface-type interface-number*]
Parameter Description	*local-ip*: inside address *global-ip*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface-type interface-number*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: name of the address pool *start-ip* start IP address *end-ip* end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: specifies the type of the NAT address pool. The rotary type is round-robin assignment and guarantees the same probability for every address to be assigned. The assignment is round-robin no matter whether **rotary** is configured or not. The parameter **rotary** is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	-

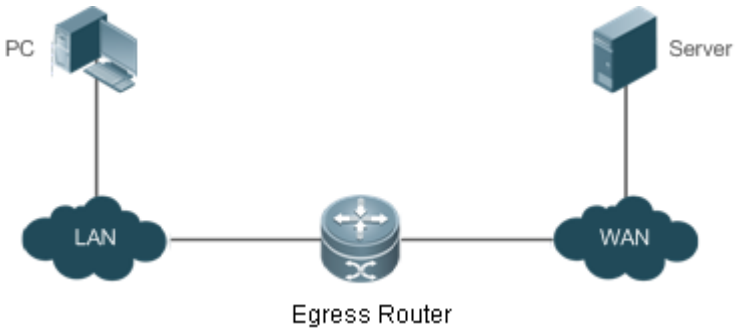
Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]
Parameter Description	*access-list-number*: ACL number **pool** *poo-namel*: name of the address pool interface *interface-type interface-number*: implements NAPT using the address of the outside global interface. **overload**: indicates that each global address in the address pool can be reused for NAPT. The global addresses are reused even if this parameter is not configured. This parameter is used to

	keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

↘ Enabling Intranet Users to Access an Extranet Server

Scenario Figure 1-5	
Configuration Steps	• Configure **ip nat inside** on the inside interface. • Configure **ip nat outside** on the outside interface. • Configure a dynamic NAT rule.
A	A# configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Verification	Use the **show** command to display the configuration.
A	Hostname# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

1.4.2 Configuring NAPT

Networking Requirements

In general, traditional NAT is one-to-one address mapping, which, however, cannot meet the requirements of all hosts in intranets to communicate with extranets. For example, when the intranet is in short of global IP addresses or even does not apply for global IP addresses but has only one global IP address to connect to an Internet Service Provider (ISP) while a large number of hosts in the intranet need to access the Internet, NAPT is required in this scenario.

Multiple inside local addresses can map to one inside global address using NAPT.

Notes

- At least one inside interface and one outside interface need to be configured for NAPT.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

↘ Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

↘ Configuring Static NAPT

- Optional configuration.
- Configure static NAPT in global configuration mode when a small number of users in the intranet need to access the extranet.

↘ Configuring Dynamic NAPT

- Optional configuration.
- Configure dynamic NAPT in global configuration mode when a large number of users in the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAPT

Command	**ip nat inside source static** { **udp** *local-ip local-port* | **tcp** *local-ip local-port* } *global-ip global-port* [**permit-inside**]
Parameter Description	**udp**: UDP **tcp**: TCP *local-ip*: inside local address *local-port*: inside local port *global-ip*: outside global address *global-port*: outside global port **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*.
Command Mode	Global configuration mode
Configuration Usage	This command is used to build an internal server that external public networks can access. Internal hosts are not allowed to access the internal server using the *global-ip* unless **permit-inside** has been configured. If **permit-inside** is not configured, internal hosts can access the internal server by using the *local-ip* only.

Configuring the Address Pool

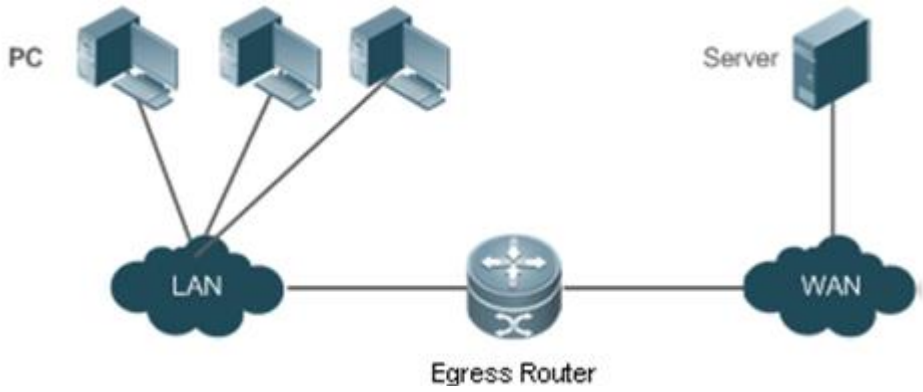
Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: name of the address pool *start-ip* start IP address *end-ip*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: specifies the type of the NAT address pool. The rotary type is round-robin assignment and guarantees the same probability for every address to be assigned. The assignment is round-robin no matter whether **rotary** is configured or not. The parameter **rotary** is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic NAPT

Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool **interface** *interface-type interface-number*: implements NAPT using the global address of the outside interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. Currently, the global addresses are reused even if this parameter is not configured. Therefore, this parameter is used only to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Enabling Intranet User to Access an Extranet Server Through NAPT

Scenario Figure 1-6	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAPT rule.
A	A# configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit

	A(config)# ip nat pool net200 200.168.12.1 200.168.12.1 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat inside source static tcp 192.168.12.3 80 200.198.12.1 80
Verification	Use the **show** command to display the configuration.
A	Hostname# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23 icmp 200.168.12.200:2064 192.168.12.66:2063 168.168.12.1:23 168.168.12.1:23 udp 200.168.12.200:2065 192.168.12.67:2063 168.168.12.1:23 168.168.12.1:23 tcp 200.168.12.200:2066 192.168.12.68:2063 168.168.12.1:23 168.168.12.1:23 tcp 200.168.12.200:2067 192.168.12.69:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

1.4.3 Configuring Overlapping NAT

Networking Requirements

When the same IP address is allocated to two private networks to interconnect with each other or the same global IP address is allocated to a private network and a public network, this situation is called address overlapping. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is in the local network. Overlapping NAT is especially designed to implement the communications between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address in the intranet, and vice versa.

Notes

- Internal source address translation must be configured before overlapping NAT is configured.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

↘ Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static Translation of Outside Source Address

- Optional configuration.
- Configure static translation of outside source address in global configuration mode when a small number of users in the extranet need to access the intranet.

Configuring Dynamic Translation of Outside Source Address

- Optional configuration.
- Configure dynamic translation of outside source address in global configuration mode when a large number of users in the extranet need to access the intranet.

Configuring an ACL

- ACL configuration is mandatory when dynamic source address mapping is used.
- Restrict the range of users requiring source address translation in the intranet.

Configuring a Static Route

- Mandatory configuration.
- Specify the network egress after inside destination address translation.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the device.

Configuring Static Translation of Outside Source Address

Command	**ip nat outside source static** *global-ip local-ip*
Parameter Description	*global-ip*: outside global address *local-ip*: inside local address
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Static Translation of Outside Source Address and Port

Command	**ip nat outside source static** { **tcp** *global-ip global-port* **|** **udp** *global-ip global-port* } *local-ip local-port*
Parameter Description	*protocol*: protocol number *global-ip*: outside global address *global-port*: outside global port *local-ip*: inside local address *local-port*: inside local port
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*poo-namel*: name of the address pool *start-ip*: start IP address *end-ip*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: specifies the type of the NAT address pool. The rotary type is round-robin assignment and guarantees the same probability for every address to be assigned. The assignment is round-robin no matter whether **rotary** is configured or not. The parameter **rotary** is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

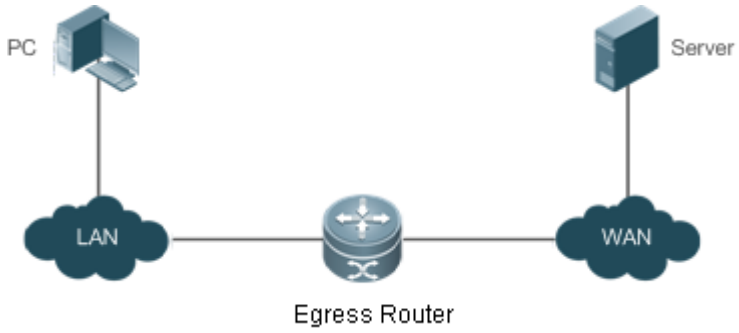
Configuring Dynamic Translation of Outside Source Address

Command	**ip nat outside source list** *access-list-number* **pool** *pool-name*
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

The following configuration example describes configuration related to static translation of outside source address.

Static Translation of Outside Source Address

Scenario **Figure 1-7**	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a rule for dynamic translation of inside source address. ● Configure a rule for static translation of outside source address.
A	A# configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat outside source static 192.168.12.3 172.16.10.1 A(config)# ip route 172.16.10.0 255.255.255.0 200.198.12.2
Verification	Use the **show** command to display the configuration.
A	Hostname# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 172.16.10.1:23 168.168.12.3:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.
- No static route is configured or no IP address is configured for the outside interface, so that the device does not know to which interface a data packet should be sent after NAT or from which interface a data packet is received after NAT.

1.4.4 Configuring TCP Load Balancing

Networking Requirements

When the TCP traffic load of an intranet host is excessively heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to attain this objective. In the following configuration, a virtual host address is defined, so that all TCP connections from extranets to the virtual host are distributed by a device to multiple physical hosts, so as to implement traffic load balancing.

Notes

The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Dynamic Translation of Inside Destination Address

- Mandatory configuration.
- Configure dynamic translation of inside destination address in global configuration mode for TCP load balancing.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the device.

Configuring the Address Pool

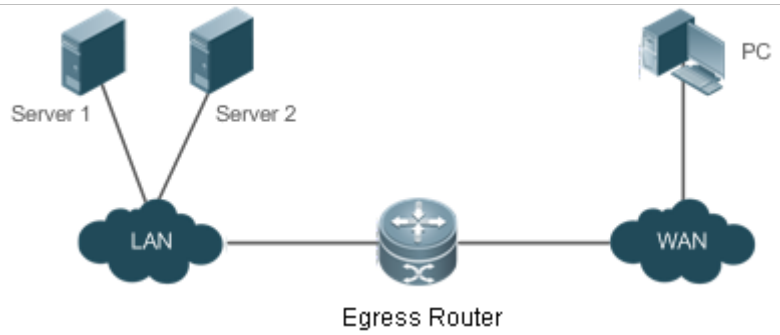
Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: name of the address pool *start-ip*: start IP address *end-ip*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: NAT address pool type. Rotary type guarantees equal chance of every address to be assigned. Whether **type rotary** is configured or not, the NAT address pool type is rotary. This parameter is introduced for compatibility with Cisco.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic Translation of Inside Destination Address

Command	**ip nat inside destination list** *access-list-number* **pool** *pool-name*
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Enabling Extranet User to Access an Intranet Server

Scenario Figure 1-8	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a rule for dynamic inside destination address translation.
A	A# configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0

	A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit A(config)# ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary A(config)# ip nat inside destination list 100 pool realhosts A(config)# access-list 100 permit ip any host 10.10.10.100
Verification	Use the **show** command to display the configuration.
A	Hostname# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 10.10.10.100:23 10.10.10.2:23 100.100.100.100:1178 100.100.100.100:1178 tcp 10.10.10.100:23 10.10.10.3:23 200.200.200.200:1024 200.200.200.200:1024

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect. Note that the ACL must be configured as an extended ACL based on destination IP address matching.
- The above configuration takes effect on TCP traffic only but not on other traffic, unless additional NAT configuration has been performed.

1.4.5 Configuring ALG

Networking Requirements

In general, NAT translates only IP address and port information in the header of a packet but does not analyze fields in the application layer data payload of the packet. However, for some special protocols, such as FTP, DNS, and FTFP, the data payloads of their packets may contain IP address or port information. If such information is not translated by NAT, certain problems may occur. The NAT ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process the IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing the correctness of application layer communications.

Notes

- At least one inside interface and one outside interface need to be configured during the configuration of ALG.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.

- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring ALG

- Optional configuration.
- The ALG configuration is mandatory if the DNS, FTP, H323, PPTP, RTSP, SIP or TFTP protocol in the environment needs to implement NAT transversal for communications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the device.

Configuring Static NAT

Command	**ip nat inside source static** *local-ip global-ip* [**permit-inside**] [**netmask** *mask* | **match** *interface-type interface-number*]
Parameter Description	*local-ip*: inside address *global-ip*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address

	match *interface-type interface-number*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: name of the address pool *start-ip*: start IP address *end-ip*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: specifies the type of the NAT address pool. The rotary type is round-robin assignment and guarantees the same probability for every address to be assigned. The assignment is round-robin no matter whether **rotary** is configured or not. The parameter **rotary** is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool interface *interface-type interface-number*: implements NAPT using the address of the outside global interface. **overload**: indicates that each global address in the address pool can be reused for NAPT. The global addresses are reused even if this parameter is not configured. This parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

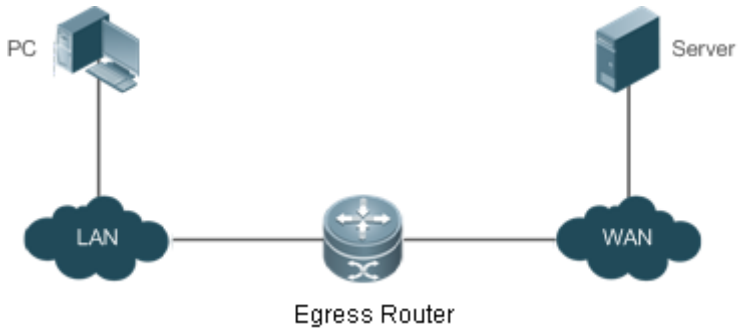
Configuring ALG

Command	**ip nat translation** { **dns** [**ttl** *ttl_time*] **| ftp** [**port** *port_num*] **| h323 | pptp | rtsp | sip | tftp** [**port** *port_num*] }
Parameter Description	**ttl**: defines the NAT timeout interval of the UDP connection of the DNS application. The default value is 0. *port_num*: The definition supports ftp and tftp port numbers. The default ftp number is 21 and the

	default tftp number is 69.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

↘ Enabling Intranet Users to Access an Extranet Server

Scenario Figure 1-9	
Configuration Steps	• Configure **ip nat inside** on the inside interface. • Configure **ip nat outside** on the outside interface. • Configure a dynamic NAT rule. • Configure ALG.
A	A# configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat translation ftp 23
Verification	Use the **show** command to display the configuration.
A	Hostname# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

1.4.6 Configuring Special NAT Applications

Networking Requirements

For some advanced applications of NAT, the source addresses or destination addresses of some specific IP packets need to be modified.

Notes

- At least one inside interface and one outside interface need to be configured for special NAT applications.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

↘ Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

↘ Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

↘ Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

↘ Configuring Special NAT Applications

- Optional configuration.
- This configuration is mandatory if special address translation is required for the communications of some applications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
CommandMode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the device.

Configuring Static NAT

Command	**ip nat inside source static** *local-ip global-ip* [**permit-inside**] [**netmask** *mask* | **match** *interface-type interface-number*]
Parameter Description	*local-ip*: inside address *global-ip*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface-type interface-number*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: name of the address pool *start-ip*: start IP address *end-ip*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: specifies the type of the NAT address pool. The rotary type is round-robin assignment and guarantees the same probability for every address to be assigned. The assignment is round-robin no matter whether **rotary** is configured or not. The parameter **rotary** is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool**

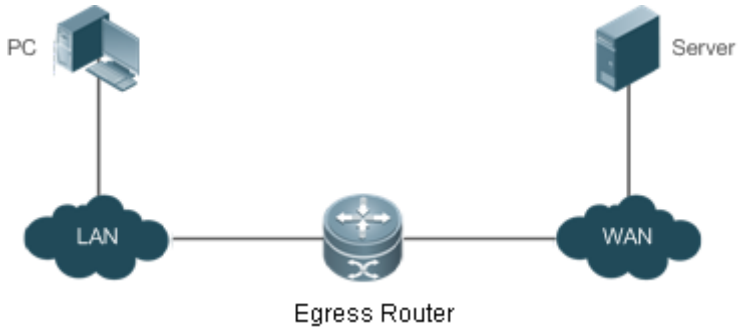
	pool-name } [**overload**]
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool interface *interface-type interface-number*: implements NAPT using the address of the outside global interface. **overload**: indicates that each global address in the address pool can be reused for NAPT. The global addresses are reused even if this parameter is not configured. This parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Special NAT Applications

Command	**ip nat application source list** *list-num* **destination** *global-ip* { **dest-change** *ip-address* | **src-change** *ip-address* }
Parameter Description	*local-ip*: inside address *global-ip*: outside address **dest-change** *ip-address port-num*: modify the destination IP address and port of the packet that satisfies conditions. **src**-change *ip-address*: modifies the source IP address of the packet that satisfies conditions.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Implementing the DNS Relay Service

Scenario Figure 1-10	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAT rule.

	• Configure special NAT applications.
A	A# configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change 202.101.98.55 53 A(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Verification	

Common Errors

- The inside or outside interface is not configured.

1.4.7 Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

Networking Requirements

Configure the interval at which gratuitous ARP packets are sent from addresses in the NAT address pool, so as to avoid address conflicts.

Notes

- Sending gratuitous ARP packets is disabled by default on the NAT device.
- Gratuitous ARP packets are sent to the outside interface only.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

↘ Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

- Optional configuration.
- NAT needs to consider some addresses matching the configured rule as local addresses. This configuration is performed to avoid address conflicts.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat** { **inside** | **outside** }
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the device.

Configuring Static NAT

Command	**ip nat inside source static** *local-ip global-ip* [**permit-inside**] [**netmask** *mask* | **match** *interface*-type interface-number]
Parameter Description	*local-ip*: inside address *global-ip*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface-type interface-number*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: name of the address pool *start-ip*: start IP address *end-ip*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: specifies the type of the NAT address pool. The rotary type is round-robin assignment and guarantees the same probability for every address to be assigned. The assignment is round-robin no matter whether **rotary** is configured or not. The parameter **rotary** is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic NAT

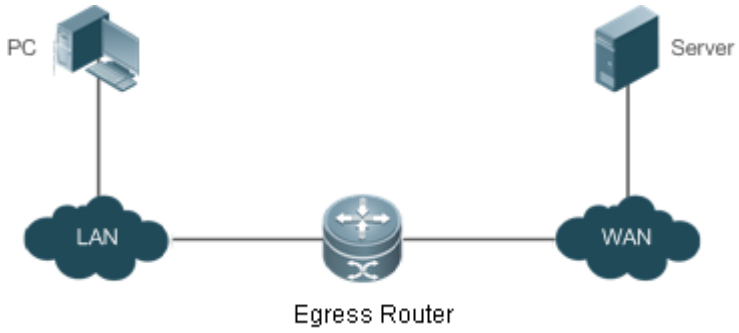
Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool interface *interface-type interface-number*: implements NAPT using the address of the outside global interface. **overload**: indicates that each global address in the address pool can be reused for NAPT. The global addresses are reused even if this parameter is not configured. This parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

Command	**ip nat keepalive** [*keealive_out*]
Parameter Description	*keealive_out*: indicates the interval at which gratuitous ARP packets are sent from the local address of NAT. The value ranges from 1 to 86,400.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Implementing the Sending of Gratuitous ARP Packets regularly

Scenario **Figure 1-11**	
Configuration Steps	• Configure **ip nat inside** on the inside interface. • Configure **ip nat outside** on the outside interface. • Configure a dynamic NAT rule. • Configure the periodical sending of gratuitous ARP packets.
A	A#configure terminal A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat inside A(config-if-GigabitEthernet 0/1)# exit A(config)# interface gigabitethernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# ip nat outside A(config-if-GigabitEthernet 0/2)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat keepalive 10
Verification	-

Common Errors

- The internal or external interface is not configured.
- NAT rule is not correct.

1.5 Monitoring

Displaying

Function	Command
Displays NAT records.	**show ip nat translations** [*dv_id*] [*slot_id*] [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

Displays NAT information based on port range.	**show ip nat user-port-range** { **configuration | users | all** }

1 Configuring DHCP

1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) is a LAN protocol based on the User Datagram Protocol (UDP) for dynamically assigning reusable network resources, for example, IP addresses.

The DHCP works in Client/Server mode. A DHCP client sends a request message to a DHCP server to obtain an IP address and other configurations. When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC3046: DHCP Relay Agent Information Option

1.2 Applications

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

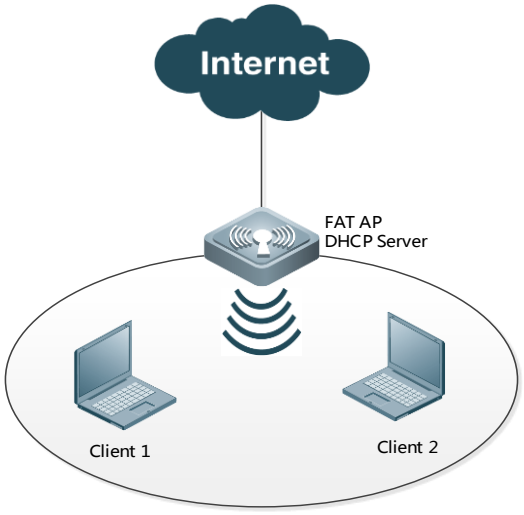
1.2.1 Providing DHCP Service in a LAN

Scenario

Assign IP addresses to two users in a LAN.

For example, assign IP addresses to Client 1 and Client 2, as shown in Figure 1-1.

Figure 1-1



Remarks	The fat AP acts as a DHCP server. Client1 and Client2 are DHCP clients.

Deployment

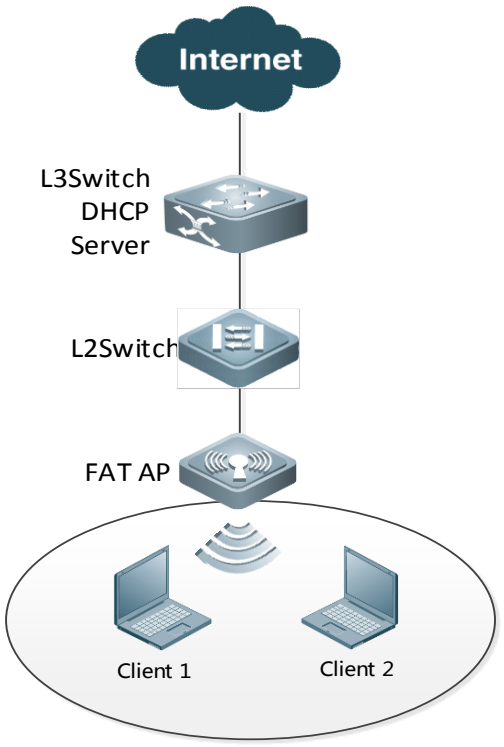
- Configure the DHCP server function on the fat AP.
- After accessing Internet, Client 1 and Client 2 initiate DHCP client requests.

1.2.2 Enabling DHCP Client

Scenario

The fat AP requests an IP address from the core switch on a LAN.

Figure 1-2



Remarks	The Layer 3 Switch is the core switch and acts as the DHCP server. Enable the DHCP client function on the fat AP.

Deployment

- Configure the DHCP server service function on the Layer 3 switch.
- Enable the DHCP client function on the uplink port of the fat AP.

1.3 Features

Basic Concepts

DHCP Server

Based on the RFC 2131, the DHCP server assigns IP addresses to clients and manages these IP addresses.

DHCP Client

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

DHCP Relay

When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Lease

Lease is a period of time specified by a DHCP server for a client to use an assigned IP address. An IP address is active when leased to a client. Before a lease expires, a client needs to renew the lease through a server. When a lease expires or is deleted from a server, the lease becomes inactive.

Excluded Address

An excluded address is a specified IP address not assigned to a client by a DHCP server.

Address Pool

An address pool is a collection of IP addresses that a DHCP server may assign to clients.

Option Type

An option type is a parameter specified by a DHCP server when it provides lease service to a DHCP client. For example, a public option include the IP addresses of a default gateway, WINS server and a DNS server. DHCP server allows configuration of other options. Though most options are defined in the RFC 2132, you can add user-defined options.

Overview

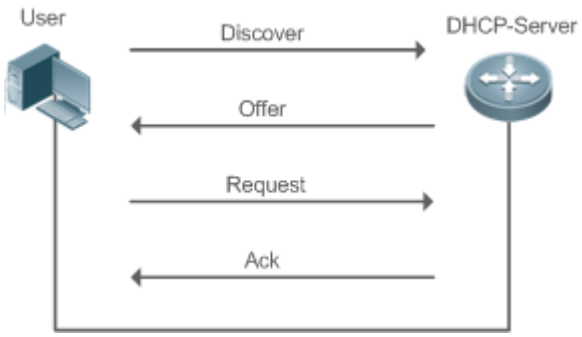
Feature	Description
DHCP Server	Enable DHCP Server on a device, and it may assign IP addresses dynamically and pushes configurations to DHCP clients.
DHCP Relay Agent	Enable DHCP Relay on a device, and it may forward DHCP request and reply packets across different network segments.
DHCP Client	Enable DHCP Client on a device, and it may obtain IP addresses and configurations automatically from a DHCP server.
Class Rule	Enable the class rule function on a device to assign IP addresses based on class rules.

1.3.1 DHCP Server

Working Principle

DHCP Working Principle

Figure 1-3



A host requests an IP address through DHCP as follows:

1. A host broadcasts a DHCP discover packet to find DHCP servers in a network.

2. DHCP servers unicast/broadcast (based on the property of the host packet) DHCP offer packets to the host, containing an IP address, a MAC address, a domain name and a lease.
3. The host broadcasts a DHCP request packet to formally request an IP address.
4. A DHCP server sends a DHCP ACK unitcast packet to the host to acknowledge the request.

A DHCP client may receive DHCPOFFER packets from multiple DHCP servers, but usually it accepts only the first DHCPOFFER packet. Besides, the address specified in a DHCPOFFER packet is not necessarily assigned. Instead, it is retained by the DHCP server until a client sends a formal request.

To formally request an IP address, a client broadcasts a DHCPREQUEST packet so that all DHCP servers sending DHCPOFFER packets may receive the packet and release OFFER IP addresses.

If a DHCPOFFER packet contains invalid configuration parameters, a client will send a DHCPDECLINE packet to the server to decline the configuration.

During the negotiation, if a client does not respond to the DHCPOFFER packets in time, servers will send DHCPNAK packets to the client and the client will reinitiate the process.

During network construction, DHCP servers have the following features:

- Low cost. Usually the static IP address configuration costs more than DHCP configuration.
- Simplified configuration. Dynamic IP address assignment dramatically simplifies device configuration
- Centralized management. You can modify the configuration for multiple subnets by simply modifying the DHCP server configuration.

Address Pool

After a server receives a client's request packet, it chooses a valid address pool, determines an available IP address from the pool through PING, and pushes the pool and address configuration to the client. The lease information is saved locally for validity check upon lease renewal.

An address pool may carry various configuration parameters as follows:

- An IP address range, which is the range of IP addresses that are available.
- A gateway address. A maximum of 8 gateway addresses are supported.
- A DNS address. A maximum of 8 DNS addresses are supported.
- A lease period notifying clients of when to age an address and request a lease renewal.

VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, Ruijie devices enabled with DHCP provide a command to monitor the VRRP status of the interface. To an interface configured with VRRP address and VRRP monitoring, a DHCP server only processes the DHCP clients' request packets from the interface in Master state, and other packets are discarded. If no VRRP address is configured, the DHCP server does not monitor the VRRP status, and all DHCP packets are processed. VRRP monitoring is configured on only layer-3 interfaces. It is disabled by default, namely, only the Master device processes the DHCP service.

IP Address Assignment Based on VLANs, Ports and IP Range

After an IP address pool is deployed, the specified IP address range is assigned based on VLANs and ports. There are three scenarios. 1. Global configuration. 2. Configuration based on VLANs, ports and IP range. 3. Both 1 and 2.

In scenario 1, the addresses are assigned globally. In scenario 2, the addresses in the specified IP range are assigned only to the clients of the specified VLANs and ports. In scenario 3, the clients of the specified VLANs and ports are assigned the addresses in the specified IP range, and the other clients are configured with default global addresses.

↘ Adding Trusted ARP

A trusted ARP prevents gateway ARP spoofing. Ruijie devices enabled with DHCP provide a command for pushing a trusted ARP while assigning an address. After this function is enabled, DHCP server pushes it while assigning an IP address to the client to prevent ARP spoofing.

↘ ARP-Based Offline Detection

Ruijie devices enabled with DHCP provide a command to enable ARP-based offline detection. After this function is enabled, a DHCP server will receive an ARP aging notification when a client gets offline, and start retrieving the client's address. If the client does not get online within a period of time (5 minutes by default), the DHCP server will retrieve the address and assign it to another client. If the client gets online again, the address is still valid.

↘ Adding Pseudo Server Detection

If a DHCP server is deployed illegally, a client interacts with this server while requesting an IP address and a wrong address will be assigned to the client. This server is a pseudo server. Ruijie devices enabled with DHCP provides a command to enable pseudo server detection. After it is enabled, DHCP packets are checked for Option 54 (Server Identifier Option). If the content of Option 54 is different from the actual DHCP server identifier, the IP address of the pseudo server and port receiving the packets will be recorded. The pseudo server detection is only an after-event security function and cannot prevent an illegal DHCP server from assigning IP addresses to clients.

↘ Preferentially Assigning the DNS Address Obtained from an External DHCP Server

When some ports on a device work in PPPoE or DHCP client mode, the ports can automatically obtain a DNS address from an external DHCP server and configure the address on the DHCP server of the local device. This eliminates the need to perform DNS configuration. When a device serves as the DHCP server, the device preferentially assigns STAs with DNS addresses obtained from an external DHCP server.

• ARP Entry Check

The ARP entry check function is a supplement to the ping conflict detection function. If there is a STA with a static IP address and Layer 2 isolation and the ping conflict detection function becomes invalid (for example, the firewall is enabled on the STA), a STA that applies for a dynamic address may be assigned with this IP address, resulting in an IP address conflict. If the ARP entry check function is enabled, the device queries its ARP entries after detecting ping conflicts of assigned IP addresses. If an ARP entry exists for the IP address to be assigned and the ARP entry is different from the MAC address of the STA for which the IP address is to be assigned, the device considers that this IP address has been occupied and will not assign it to another STA.

If there are ARP attacks, you are advised to disable the ARP entry check function. Otherwise, the DHCP assignment service is affected. As a result, it takes a long time for a STA to apply for an IP address or the STA cannot apply for an IP address.

Related Configuration

Enabling DHCP Server Globally

- By default, DHCP Server is disabled.
- Run the **service dhcp** command to enable the DHCP Server.
- Run the **service dhcp** command globally to enable DHCP service.

Configuring Address Pool

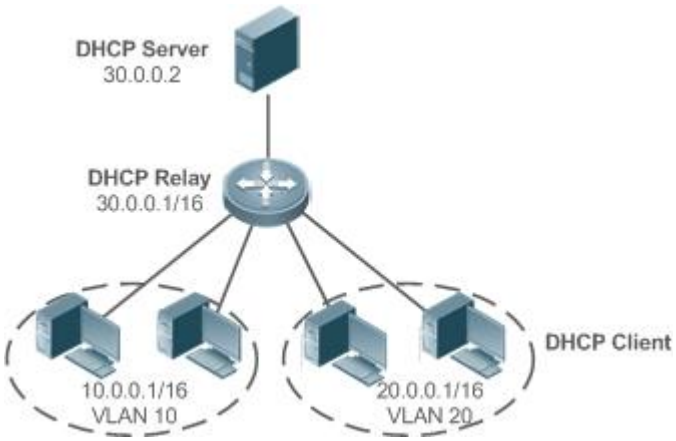
- By default, no address pool is configured.
- Run the **ip dhcp pool** command to configure an IP address range, a gateway and a DNS.
- If no address pool is configured, no addresses will be assigned.

1.3.2 DHCP Relay Agent

Working Principle

The destination IP address of DHCP request packets is 255.255.255.255, and these packets are forwarded within a subnet. To achieve IP address assignment across network segments, a DHCP relay agent is needed. The DHCP relay agent unicasts DHCP request packets to a DHCP server and forwards DHCP reply packets to a DCHP client. The DHCP relay agent serves as a repeater connecting a DHCP client and a DHCP server of different network segments by forwarding DHCP request packets and DHCP reply packets. The Client-Relay-Server mode achieves management of IP addresses across multiple network segments by only one DHCP server. See the following figure.

Figure 1-4 DHCP Relay Scenario



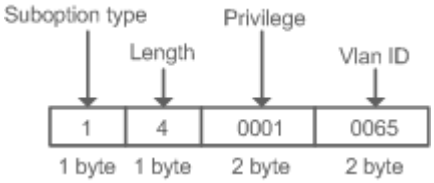
VLAN 10 and VLAN 20 correspond to the segments 10.0.0.1/16 and 20.0.0.1/16 respectively. A DHCP server with IP address 30.0.0.2 is in segment 30.0.0.1/16. To achieve management of dynamic IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable DHCP Relay on a gateway and configure IP address 30.0.0.2 for the DHCP server.

DHCP Relay Agent Information (Option 82)

As defined in RFC3046, an option can be added to indicate a DHCP client's network information when DHCP Relay is performed, so that a DHCP server may assign IP addresses of various privileges based on more accurate information. The option is called Option 82. There are four types of relay agent information:

a) Relay agent information option dot1x: This scheme should be implemented with 802.1X authentication and an authentication server. A DHCP relay agent constructs the **Circuit ID** sub-option based on the IP privilege delivered during 802.1X authentication and the VID of a DHCP client. The option format is shown in Figure 1-5.

Figure 1-5 Option Format



b) Relay agent information option82: This scheme serves without correlation with other protocol modules. A DHCP relay agent forms an Option 82 based on the physical port receiving DHCP request packets and the MAC address of the device. The option format is shown in the following figure.

Figure 1-6Agent Circuit ID

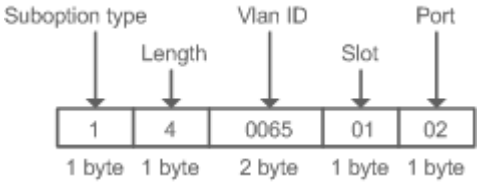
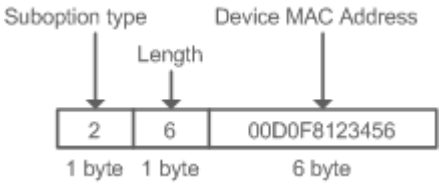


Figure 1-7 Agent Remote ID



c) Relay agent information Option 82: This scheme serves without correlation with other protocol modules. Compared with previous Option 82, the option supports custom content, which may change. By default, a DHCP relay agent forms Option 82 based on the information of the physical port receiving DHCP packets, device MAC address and device name. The option format is shown in the following figure.

Figure 1-8 Option 82-circuit-id

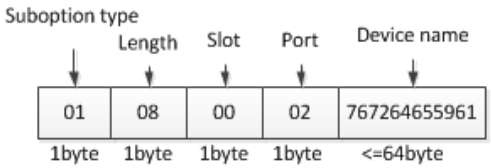
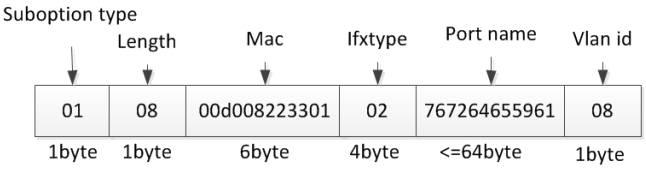


Figure 1-9 Option 82-remote-id



DHCP Relay Check Server-ID

- In DHCP environment, multiple DHCP servers are deployed for a network, achieving server backup to ensure uninterrupted network operation. After this function is enabled, the DHCP request packet sent by a client contains a **server-id** option specifying a DHCP server. In alleviating the burden on servers in specific environments, you need to enable this function on a relay agent to send a packet to a specified DHCP server rather than all DHCP servers.

Related Configuration

Enabling DHCP Relay

- By default, DHCP Relay is disabled.
- You may run the **service dhcp** command to enable DHCP Relay.
- You need to enable DHCP Relay before it works.

Configuring IP Address for DHCP Server

- By default, no IP address is configured for a DHCP server.
- You can run the **ip helper-address** command to configure an IP address for a DHCP server. The IP address can be configured globally or on a Layer 3 interface. A maximum of 20 DHCP server addresses can be globally configured or configured on each Layer 3 interface.
- When an interface receives a DHCP request packet, the DHCP server list on the interface takes effect first. If the interface is not configured with a DHCP server list, the global DHCP server list takes effect.

Enabling DHCP Option 82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable DHCP Option 82.

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Forcing a DHCP Relay to Send Reply Messages

- By default, a DHCP Relay is not forced to send reply messages.
- Run the **ip dhcp relay force-send-reply-pack** command to force a DHCP Relay to send reply messages.

1.3.3 DHCP Client

Working Principle

A DHCP client broadcasts a DHCP discover packet after entering the Init state. Then it may receive multiple DHCP offer packets. It chooses one of them and responds to the corresponding DHCP server. After that, it sends lease renewal request packets in the Renew and Rebind processes of an aging period to request lease renewal.

Related Configuration

Enabling DHCP Client on Interface

- By default, DHCP Client is disabled.
- In interface configuration mode, you may run the **ip address dhcp** command to enable DHCP Client.
- You need to enable DHCP Client to enable DHCP service.
- The configuration takes effect on a layer-3 interface, for example, an SVI or a routed port.

Defining Common Option Fields on Interfaces

- In interface configuration mode, run the **ip dhcp client class-id** command to define the option61 field in request messages.
- In interface configuration mode, run the **ip dhcp client client-id** command to define the option60 field in request messages.
- In interface configuration mode, run the **ip dhcp client hostname** command to define the option12 field in request messages.
- In interface configuration mode, run the **ip dhcp client lease** command to define the oprion51 field in request messages.
- In interface configuration mode, run the **ip dhcp client option-list** command to define the option55 field in request messages.
- The configuration takes effect on a Layer 3 interface only, for example, an SVI or a routed port.

Releasing and Renewing a DHCP Lease

- In privilege EXEC configuration mode, run the **release-dhcp** command to release a DHCP lease.
- In privilege EXEC configuration mode, run the **renew-dhcp** command to renew a DHCP lease.

1.3.4 Class Rule

Working Principle

When STAs apply for IP addresses from different APs, Option 82 information carried by the STAs is different. The class rules are used to match the Option 82 information to assign IP addresses in different network segments to STAs.

Related Configuration

Configuring Class Rules in Global Configuration Mode

- Run the **ip dhcp class** command to add class rules.
- Run the **relay agent information** command to enter the Option 82 configuration mode.
- Run the **relay-information hex** command to configure matched Option 82 content.

Associating Configured Class Rules in Address Pool Configuration Mode

- Run the **class** command to associate class rules.
- Run the **address range** command to configure assigned IP address segments after class rules are matched.

1.4 Configuration

Configuring DHCP Server

Configuration	Description and Command	
Configuring Dynamic IP Address	⚠ (Mandatory) It is used to enable DHCP Server to achieve dynamic IP address assignment.	
	service dhcp	Enables DHCP Server.
	ip dhcp pool	Configures an address pool.
	network	Configures the network number and subnet mask of a DHCP address pool.
	⚠ (Optional) It is used to configure the properties of an address pool.	
	address range	Configures the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool.
	default-router	Configures a default gateway of a client.
	lease	Configures an address lease.
	next-server	Configures a TFTP server address
	bootfile	Configures a boot file of a client.
	domain-name	Configures a domain name of a client.
	dns-server	Configures a domain name server.
	netbios-name-server	Configures a NetBIOS WINS server.
	netbios-node-type	Configures a NetBIOS node type on a client.
	lease-threshold	Configures an alarm threshold of an address pool.
	option	Configures a user-defined option.
	pool-status	Enables or disables an address pool.
	force-no-router	Cancels gateway allocation to the client
	class	Configure class rules to be matched
	address range	Configures assigned IP network segments after the class rules are matched.
Configuring Static IP Address	⚠ (Optional) It is used to statically assign an IP address to a client.	

Configuration	Description and Command	
	ip dhcp pool	Configures an address pool name and enters address pool configuration mode.
	host	Configures the IP address and subnet mask of a client host.
	hardware-address	Configures a client hardware address.
	client-identifier	Configures a unique client identifier.
	client-name	Configures a client name.
Configuring Global Properties of DHCP Server	⚠ (Optional) It is used to configure the properties of a DHCP server.	
	ip dhcp excluded-address	Configures an excluded IP address.
	ip dhcp force-send-nak	Configures Compulsory NAK reply by a DHCP server.
	ip dhcp monitor-vrrp-state	Configures VRRP status monitoring.
	ip dhcp ping packets	Configures ping times.
	ip dhcp ping timeout	Configures a ping timeout.
	ip dhcp refresh arp	Configures a DHCP server to refresh trusted ARPs.
	ip dhcp server detect	Configures pseudo server detection.
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode
	ip dhcp use class	Enables the CLASS to allocate addresses in the global configuration mode.

↘ Configuring DHCP Relay

Configuration	Description and Command	
Configuring Basic DHCP Relay Functions	⚠ (Mandatory) It is used to enable DHCP Relay.	
	service dhcp	Enables DHCP Relay.
	ip helper-address	Configures an IP Address of a DHCP Server.
Configuring DHCP Relay Option 82	⚠ (Optional) It is used to assign IP addresses of different privileges to clients in combination with the information of a physical port. This function cannot be used together with the **dhcp option dot1x** command.	
	ip dhcp relay information option82	Enables DHCP option82.
Configuring DHCP Relay Check Server-ID	⚠ (Optional) It is used to enable a DHCP Relay agent to send DHCP request packets only to a specified server.	
	ip dhcp relay check server-id	Enables a DHCP Relay agent to send DHCP request packets only to a specified server

Configuring DHCP 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.
Defining Fields in Request Messages on Interfaces	(Optional) It is used to define common option fields to configure the DHCP client function.	
	ip dhcp client class-id	Defines information in **class id**
	ip dhcp client client-id	Defines information in **client id**
	ip dhcp client hostname	Defines information in **hostname**
	ip dhcp client lease	Defines information in **lease**
	ip dhcp client option-list include	Defines information in **option-list**
Releasing and Renewing DHCP Leases	(Optional) It is used to define common option fields to configure the DHCP client function.	
	release-dhcp	Enables a DHCP client to release IP addresses.
	renew-dhcp	Enables a DHCP client to renew IP addresses.

Configuring Class Rules

Configuration	Description and Command	
Configuring Class Rules of the DHCP Server	(Optional) It is used to configure class rules.	
	ip dhcp class	Configures global class rules.
	ip dhcp use class	Configures address assignment based on class rules.
	relay agent information	Enters the Option 82 configuration mode.
	relay-information hex	Configures the Option 82 information matched with class rules.

1.4.1 Configuring Dynamic IP Address

Configuration Effect

Provide all DHCP Clients with DHCP service including assigning IP addresses and gateways.

Notes

A DHCP server and a DHCP relay share the **service dhcp** command, but a device cannot function as a DHCP server and relay at the same time. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuration Steps

Enabling DHCP Server

- Mandatory. It achieves dynamic IP address assignment.
- Run the **service dhcp** command in global configuration mode.

Configuring Address Pool

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

- Mandatory. It defines a range of dynamically assigned addresses.
- Run the **network** command in DHCP address pool configuration mode.

Configuring Default Gateway of Client

- Optional. It is used to configure a gateway address.
- Run the **default-router** command in DHCP address pool configuration mode.

Configuring Address Lease

- Optional. It is used to configure an IP address lease, which is 24h by default.
- Run the **lease** command in DHCP address pool configuration mode.

Configuring TFTP Server Address

- Optional. It is used to configure a TFTP server address.
- Run the **next-server** command in DHCP address pool configuration mode.

Configuring Domain Name of Client

- Optional. It is used to configure the domain name of a client.
- Run the **domain-name** command in DHCP address pool configuration mode.

Configuring DNS

- Optional. It is used to configure a DNS address.
- Run the **dns** command in DHCP address pool configuration mode.

Configuring NetBIOS WINS Server

- Optional. It is used to configure a NetBIOS WINS server address.
- Run the **netbios-name-server** command in DHCP address pool configuration mode.

Configuring NetBIOS Node Type on Client

- Optional. It is used to configure a NetBIOS node type.
- Run the **netbios-name-type** command in DHCP address pool configuration mode.

Configuring Alarm Threshold of Address Pool

- Optional. It is used to manage the number of leases. When a threshold (90% by default) is reached, an alarm will be printed.
- Run the **lease-threshold** command in DHCP address pool configuration mode.

Configuring User-Defined Option

- Optional. It is used to configure user-defined options.
- Run the **option** command in DHCP address pool configuration mode.

Enabling or Disabling Address Pool

- Optional. It is used to enable or disable an address pool. It is enabled by default.
- Run the **pool-status** command in DHCP address pool configuration mode.

Adding Trusted ARP

- Optional. It is used to add a trusted ARP while assigning an IP address. It is disabled by default.
- Run the **update arp** command in DHCP address pool configuration mode.

Refraining from Assigning Gateway Address

- Optional. It is used to refrain from assigning a gateway while assigning IP address to a client. It is disabled by default.
- Run the **force-no-router** command in DHCP address pool configuration mode.

Verification

Connect a DHCP client and a DHCP server.

- Check whether the client obtains configurations on the server.

Related Commands

Configureing the Network Segment Range of the Addresses That can be Allocated by CLASS Associated with DHCP Address Pool

Command	**address range** *low-ip-address high-ip-address*
Parameter Description	*low-ip-address:* Indicates th start address in the network segment range. *high-ip-address:* Indicates the end address in the network segment range.
Command Mode	Global configuration mode
Usage Guide	Enable DHCP Server and DHCP Relay. A DHCP server and a DHCP relay share the **service dhcp** command. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Enabling DHCP Server

Command	**service dhcp**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	Enable DHCP Server and DHCP Relay. A DHCP server and a DHCP relay share the **service dhcp** command. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter DHCP address pool configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

Command	**network** *network-number mask* [*low-ip-address high-ip-address*]
Parameter Description	*network-number:* Indicates the network number of an IP address pool. *mask:* Indicates the subnet mask of an IP address pool. If no subnet mask is defined, the natural subnet mask is applied.
Command Mode	DHCP address pool configuration mode
Usage Guide	To configure dynamic address assignment, you need to configure a network number and subnet mask of an address pool to provide a DHCP server with a range of addresses. The IP addresses in a pool are assigned in order. If an address is assigned or exists in the target network segment, the next address will be checked until a valid address is assigned. It provides available network segments by specifying start and end addresses. The configuration is optional. If the start and end address are not specified, all IP addresses in the network segment are assignable. Addresses are assigned based on the client's physical address and ID. Therefore, one client will not be assigned two leases from one address pool. In case of topological redundancy between a client and a server, address assignment may fail. To avoid such failures, a network administrator needs to prevent path redundancy in network construction, for example, by adjusting physical links or network paths.

Configuring Default Gateway of Client

Command	**default-router** *address* [*address2…address8*]
Parameter Description	*address*: Indicates the IP address of a default gateway. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 gateways can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure a default gateway of a client, and a server will push the gateway configuration to the client. The IP addresses of the default gateway and the client should be in a same network.

Configuring Address Lease

Command	**lease** {*days* [*hours]* [*minutes*] | **infinite**}
Parameter Description	*days:* Defines a lease in the unit of day. *hours:* (Optional) Defines a lease in the unit of hour. Please define *days* before *hours*. *minutes:* (Optional) Defines a lease in the unit of minute. Please define *days* and *hours* before *minutes*. **infinite:** Defines an unlimited lease.
Command Mode	DHCP address pool configuration mode
Usage Guide	The default lease of an IP address assigned by a DHCP server is 1 day. When a lease is expiring soon, a client needs to request a lease renewal. Otherwise the IP address cannot be used after the lease is expired.

Configuring IP Addresses of Boot Servers for Clients

Command	**next-server** *ip-address* [*ip-address2...ip-address8*]
Parameter Description	*ip-address*: defines the IP address of a boot server, typically a TFTP server. You need to configure at least one boot server. *ip-address2...ip-address8*: indicates IP addresses of boot servers, which is optional. You can configure up to eight boot servers.
Command Mode	DHCP address pool configuration mode
Usage Guide	Run this command to configure servers. When multiple boot servers are defined, the first defined boot server has the highest priority. A DHCP client selects the next boot server only when it fails to communicate with the first defined boot server.

Configures Boot File on Client

Command	**bootfile** *filename*
Parameter Description	*file-name*: Defines a boot file name.
Command Mode	DHCP address pool configuration mode
Usage Guide	A boot file is a bootable image file used when a client starts up. The file is usually an OS downloaded by a DHCP client.

Configuring Domain Name of Client

Command	**domain-name** *domain*
Parameter Description	*domain-name:* Defines a domain name of a DHCP client.
Command Mode	DHCP address pool configuration mode
Usage Guide	You may define a domain name for a client. When the client accesses network through the host name, the domain name will be added automatically to complete the host name.

Configuring DNS

Command	**dns-server** *ip-address* [*ip-address2...ip-address8*]
Parameter Description	*ip-address:* Defines an IP address of a DNS server. Configure at least one IP address. *ip-address2...ip-address8:* (Optional) A maximum of 8 DNS servers can be configured. **use-dhcp-client** *interface-type interface-number:* A DHCP client learns its DNS server via RGOS software.
Command Mode	DHCP address pool configuration mode
Usage Guide	If a client accesses network resources through the domain name, you need to configure a DNS server to resolve the domain name.

Configuring NetBIOS WINS Server

Command	**netbios-name-server** *address* [*address2...address8*]
Parameter Description	*address:* Defines an IP address of a WINS server. Configure at least one IP address. *ip-address2...ip-address8:* (Optional) A maximum of 8 WINS servers can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	WINS is a domain name service through which a Microsoft TCP/IP network resolves a NetNBIOS name to an IP address. A WINS server is a Windows NT server. When a WINS server starts, it receives a registration request from a WINS client. When the client shuts down, it sends a name release message, so that the computers in the WINS database and on the network are consistent.

Configuring NetBIOS Node Type on Client

Command	**netbios-node-type** *type*
Parameter Description	type: Defines a NetBIOS node type with one of the following approaches. 1. A hexadecimal number, ranging from 0 to FF. Only followings values are available. ● 1 for b-node ● 2 for p-node ● 4 for m-node ● 8 for h-node 2. A character string. ● b-node for a broadcast node; ● p-node for a peer-to-peer node; ● m-node for a mixed node; ● h-node for a hybrid mode.
Command Mode	DHCP address pool configuration mode
Usage Guide	There are four types of NetBIOS nodes of a Microsoft DHCP client. 1) A broadcast node. For such a node, NetBIOS name resolution is requested through broadcast.2) A peer-to-peer node. The client sends a resolution request to the WINS server. 3) A mixed node. The client broadcasts a resolution request and sends the resolution request to the WINS server 4) A hybrid node. The client sends a resolution request to the WINS server. If no reply is received, the client will broadcast the resolution request. By default, a Microsoft operating system is a broadcast or hybrid node. If no WINS server is configured, it is a broadcast node. Otherwise, it is a hybrid node.

Configuring the Alarm Threshold of an Address Pool

Command	lease-threshold percentage
Parameter Description	percentage: defines the percentage threshold of an address pool alarm. The value ranges from 60 to 100.
Command Mode	DHCP address pool configuration mode
Usage Guide	Run this command to configure servers. When the IP address usage of an address pool reaches the threshold, a DHCP server generates Syslog alarms. The IP address usage is the ratio of assigned IP addresses to available IP addresses in an address pool. If the number of assigned IP addresses exceeds the alarm threshold, one alarm is generated every five minutes.

Configuring User-Defined Option

Command	**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }
Parameter Description	*code:* Defines a DHCP option code. **ascii** *string:* Defines an ASCII character string. **hex** *string:* Defines a hexadecimal character string. **ip** *ip-address:* Defines an IP address.
Command Mode	DHCP address pool configuration mode
Usage Guide	The DHCP allows transmitting configuration information to a host via a TCP/IP network. DHCP packets contain the option field of definable content. A DHCP client should be able to receive a DHCP packet carrying at least 312 bytes option. Besides, the fixed data field in a DHCP packet is also called an option. In a WLAN, a DHCP client on an AP dynamically requests the IP address of an AC. You may configure on a DHCP server the **option** command specifying the AC address.

Enabling or Disabling Address Pool

Command	**pool-status** {**enable | disable**}
Parameter Description	**enable***:* Enables an address pool. **disable***:* Disable an address pool. It is enabled by default.
Command Mode	DHCP address pool configuration mode
Usage Guide	You can run the command to enable or disable this service of a DHCP address pool.

Adding Trusted ARP

Command	**update arp**
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	After configuration, a trusted ARP is added when an address is assigned from a pool. A trusted ARP prevents ARP spoofing.

Refraining from Assigning Gateway Address

Command	force-no-router
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	If a client requests an IP address as well as a gateway address, a DHCP server assigns an IP address and a gateway address to the client. After configuration, no gateway address is sent to the client.

Configuration Example

Configuring Address Pool

Configuration Steps	● Define an address pool net172. ● The network segment is 172.16.1.0/24. ● The default gateway is 172.16.1.254. ● The address lease is 1 day. ● xcluded addresses range from 172.16.1.2 to 172.16.1.100.
	Hostname(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100 Hostname(dhcp-config)# ip dhcp pool net172 Hostname(dhcp-config)# network 172.16.1.0 255.255.255.0 Hostname(dhcp-config)# default-router 172.16.1.254 Hostname(dhcp-config)# lease 1
Verification	● Run the **show running-config** command to display the configuration.
	Hostname#show running-config | begin ip dhcp ip dhcp excluded-address 172.16.1.2 172.16.1.100 ip dhcp pool net172 network 172.16.1.0 255.255.255.0default-router 172.16.1.254 lease 1

1.4.2 Configuring Static IP Address

Configuration Effect

Assign specific IP addresses and push configuration to specific DHCP clients.

Notes

N/A

Configuration Steps (A)

Configuring Address Pool Name and Entering Address Pool Configuration Mode

- Mandatory. It is used to create an IP address pool.

- Run the **ip dhcp pool** command in global configuration mode.

Configuring IP Address and Subnet Mask of Client

- Mandatory. It is used to configure a static IP address and a subnet mask.
- Run the **host** command in DHCP address pool configuration mode.

Configuring Hardware Address of Client

- Optional. It is used to configure a MAC address.
- Run the **hardware** command in DHCP address pool configuration mode.

Configures Unique Client Identifier

- Optional. It is used to configure a static user identifier (UID).
- Run the **client-identifier** command in DHCP address pool configuration mode.

Configuring Client Name

- Optional. It is used to configure a static client name.
- Run the **host-name** command in DHCP address pool configuration mode.

Verification

Check whether the client obtains the IP address when it is online.

Related Commands

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter address pool configuration mode.

Manual IP Address Binding

Command	**host** *ip-address* [*netmask*] **client-identifier** *unique-identifier* **client-name** *name*
Parameter Description	*ip-address:* Defines the IP address of a DHCP client. *netmask:* Defines the subnet mask of a DHCP client. *unique-identifier:* Defines the hardware address (for example, aabb.bbbb.bb88) and identifier (for example, 01aa.bbbb.bbbb.88) of a DHCP client. *name:* (Optional) It defines a client name using ASCII characters. The name excludes a domain name. For example, name a host **mary** rather than **mary.rg.com**.
Command	DHCP address pool configuration mode

Mode	
Usage Guide	Address binding means mapping between an IP address and a client's MAC address. There are two kind of address binding. 1) Manual binding. Manual binding can be deemed as a special DHCP address pool with only one address. 2) Dynamic binding. A DHCP server dynamically assigns an IP address from a pool to a client when it receives a DHCP request, creating mapping between the IP address and the client's MAC address. To configure manual binding, you need to define a host pool and then specify a DHCP client's IP address and hardware address or identifier. A hardware address is a MAC address. A client identifier includes a network medium type and a MAC address. A Microsoft client is usually identified by a client identifier rather than a MAC address. For the codes of medium types, refer to the *Address Resolution Protocol Parameters* section in the RFC 1700. The Ethernet type is **01**.

Configuring Client Hardware Addresses

Command	**hardware-address** *hardware-address* [*type*]
Parameter Description	*hardware*-address: indicates the MAC address of a DHCP client *type*: identifies the hardware platform protocol of a DHCP client. The value can be a character string or number. Character string options: ● ethernet ● ieee802 Number options: ● 1 (10 M ethernet) ● 6 (IEEE 802)
Command Mode	DHCP address pool configuration mode
Usage Guide	Run this command to configure servers. This command can be used only when you assign a static IP addresses manually.

Configuration Example

Dynamic IP Address Pool

Configuration Steps	● Configure address pool VLAN 1 with IP address 20.1.1.0 and subnet mask 255.255.255.0. ● The default gateway is 20.1.1.1. ● The lease time is 1 day.
	Hostname(config)# ip dhcp pool vlan1 Hostname(dhcp-config)# network 20.1.1.0 255.255.255.0 Hostname(dhcp-config)# default-router 20.1.1.1 Hostname(dhcp-config)# lease 1 0 0
Verification	● Run the **show running-config** command to display the configuration.
	Hostname#show running-config | begin ip dhcp ip dhcp pool vlan1

	network 20.1.1.0 255.255.255.0 default-router 20.1.1.1 lease 1 0 0

Manual Binding

Configuration Steps	● The host address is 172.16.1.101 and the subnet mask is 255.255.255.0. ● The host name is Billy.rg.com. ● The default gateway is 172.16.1.254. ● The MAC address is 00d0.df34.32a3.
	Hostname(config)# ip dhcp pool Billy Hostname(dhcp-config)# host 172.16.1.101 255.255.255.0 Hostname(dhcp-config)# client-name Billy Hostname(dhcp-config)# hardware-address 00d0.df34.32a3 Ethernet Hostname(dhcp-config)# default-router 172.16.1.254
Verification	● Run the **show running-config** command to display the configuration.
	Hostname#show running-config | begin ip dhcp ip dhcp pool Billy host 172.16.1.101 255.255.255.0 client-name Billy hardware-address 00d0.df34.32a3 Ethernet default-router 172.16.1.254

Configuration Steps (B)

Configuring an Address Pool Name and Entering the Address Pool Configuration Mode

- (Mandatory.) It is used to create an IP address pool.
- Run the **ip dhcp pool** command in address pool configuration mode.

Verification

- Check whether the client obtains the IP address when it is online.

Related Commands

Configuring an Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter the address pool configuration mode.

1.4.3 Configuring Global Properties of DHCP Server

Configuration Effect

Enable a server with specific functions, for example, ping and compulsory NAK.

Notes

Configuring the command may cause exceptions on other servers.

Configuration Steps

Configuring Excluded IP Address

- Optional. Configure some addresses or address ranges as unavailable.
- Run the **ip dhcp excluded-address** command in global configuration mode.

Configuring Compulsory NAK Reply

- Optional. A server replies to a wrong address request with a NAK packet.
- Run the **ip dhcp force-send-nak** command in global configuration mode.

Configuring VRRP Status Monitoring

- Optional. After configuration, DHCP packets are processed by the Master server.
- Run the **ip dhcp monitor-vrrp-state** command in global configuration mode.

Configuring Ping Times

- Optional. Check the address reachability with the **ping** command. The default is 2.
- Run the **ip dhcp ping packet** command in global configuration mode.

Configuring Ping Timeout

- Optional. Check the address reachability with the **ping** command. The default is 500 ms.
- Run the **ip dhcp ping timeout** command in global configuration mode.

Refreshing Trusted ARP

- Configure a DHCP server to refresh trusted ARPs according to the addresses assigned from an address pool configured with the **update arp** command.
- Run the **ip dhcp refresh arp** command in global configuration mode.

Configuring Pseudo Server Detection

- Optional. Enable this function to log a pseudo server.
- Run the **ip dhcp server detect** command in global configuration mode.

Verification

Run the **dhcp-server** command, and check the configuration during address assignment.

Related Commands

Configuring Excluded IP Address

Command	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address:* Indicates a start IP address. *high-ip-address:* Indicates an end IP address.
Command Mode	Global configuration mode
Usage Guide	Unless otherwise specified, a DHCP server assigns all the addresses from an IP address pool to DHCP clients. To reserve some addresses(e.g., addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, it is recommended to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.

Configuring Compulsory NAK Reply

Command	**ip dhcp force-send-nak**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In a WLAN, a DHCP client often moves from one network to another. When a DHCP server receives a lease renewal request from a client but finds that the client crosses the network segment or that the lease is expired, it replies with a NAK packet to require the client to obtain an IP address again. This prevents the client from sending request packets continually before obtaining an IP address again after timeout. The server sends a NAK packet only when it finds the client's lease record. When a DHCP client crosses the network, a DHCP server cannot find lease record of the client and will not reply with a NAK packet. The client sends request packets continually before obtaining an IP address again after timeout. Consequently, it takes a long to obtain an IP address. This also occurs when a DHCP server loses a lease after restart and a client requests lease renewal. In this case, you may configure a command to force the DHCP server to reply with a NAK packet even though it cannot find the lease record so that the client may obtain an IP address rapidly. Please note that the command is disabled by default. To enable it, only one DHCP server can be configured in a broadcast domain.

Configuring Ping Times

Command	**ip dhcp ping packets** [*number*]
Parameter Description	*number:* (Optional) Ranges from 0 to 10. 0 indicates the ping function is disabled. The default is two pings.
Command Mode	Global configuration mode
Usage Guide	By default, when a DHCP server assigns an IP address from a pool, it runs the **Ping** command twice (one packet per time). If there is no reply, the server takes the address as idle and assigns it to a client. If there is a reply, the server takes the address as occupied and assigns another

	address.

Configuring Ping Timeout

Command	**ip dhcp ping timeout** *milliseconds*
Parameter Description	*milli-seconds:* Indicates the time that it takes for a DHCP server to wait for a ping reply. The value ranges from 100 ms to 10,000 ms.
Command Mode	Global configuration mode
Usage Guide	By default, if a DHCP server receives no Ping reply within 500 ms, the IP address is available. You may adjust the ping timeout to change the time for a server to wait for a reply.

Refreshing Trusted ARP

Command	**ip dhcp refresh arp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, if an address pool is configured with the **update arp** command, a DHCP server will refresh trusted ARPs while assigning an IP address from the address pool. If a client clears the trusted ARPs, the server will not reassign them. After configuration, a DHCP server may refresh trusted ARPs according to addresses assigned from an address pool configured with **update arp**.

Configuring Pseudo Server Detection

Command	**ip dhcp server detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, pseudo server detection is disabled on a DHCP server. Run this command to enable pseudo server detection.

Configuring a CLASS

Command	**ip dhcp class** *class-name*
Parameter Description	*class-name:* Class name, which can be a character string or numeric such as myclass or 1.
Command Mode	Global configuration mode
Usage Guide	After executing this command, it enters the global CLASS configuration mode which is shown as "**Ruijie (config-dhcp-class)#**". In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

Enabling the CLASS to Allocate Addresses

Command	**ip dhcp use class**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	This command is configured on the DHCP server.

Configuration Example

Configuring Ping

Configuration Steps	● Set ping times to 5. ● Set ping timeout to 800ms.
	Hostname(config)# ip dhcp ping packet 5 Hostname(config)# ip dhcp ping timeout 800
Verification	● Run the **show running-config** command to display the configuration.
	Hostname#show running-config | begin ip dhcp ip dhcp ping packet 5 ip dhcp ping timeout 800

Configuring Excluded IP Address

Configuration Steps	● Configure the excluded IP address from 192.168.0.0 to 192.168.255.255.
	Hostname(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
Verification	● Run the **show running-config** command to display the configuration.
	Hostname#show running-config | begin ip dhcp ip dhcp excluded-address 192.168.0.0 192.168.255.255

1.4.4 Configuring Basic DHCP Relay Functions

Configuration Effect

- Deploy dynamic IP management in Client–Relay–Server mode to achieve communication between a DHCP client and a DHCP server, which are in different network segments.

Notes

- To enable DHCP Relay, you need to configure IPv4 unicast routing in a network.

Configuration Steps

Enabling DHCP Relay

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Configuring IP Address for DHCP Server

- Mandatory.
- You need to configure an IP address for a DHCP server.

Verification

- Check whether a client obtains an IP address through DHCP Relay.

Related Commands

Enabling DHCP Relay

Command	service dhcp
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring IP Address for DHCP Server

Command	ip helper-address { cycle-mode | *A.B.C.D* }
Parameter Description	**cycle-mode**: Indicates that DHCP request packets are forwarded to all DHCP servers. Whether the parameter is available depends on interface modes. *A.B.C.D*: Indicates the IP address of a server.
Command Mode	Global configuration mode
Usage Guide	The configured interface must be a Layer 3 interface, such as a routed port, SVI, and loopback interface. The configured interface must be reachable through IPv4 unicast routing.

1.4.5 Configuring DHCP Relay Option 82

Configuration Effect

- Through a DHCP relay agent, a server may assign IP addresses of different privileges to the clients more accurately based on the option information.

Notes

- You need to enable the DHCP Relay function.

Configuration Steps

Enabling Basic DHCP Relay Functions

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Enables DHCP Option82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable or disable DHCP Option 82.

Verification

- Check whether the client obtains an IP address based on Option 82.

Related Commands

Enabling DHCP Option 82

Command	ip dhcp relay information option82
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When you configure the **ip dhcp relay information option82** command, the device acts as a DHCP relay agent. The device adds Option 82 to a DHCP request packet to be forwarded to a DHCP server. The encapsulation format of **circuit-id** is "slot(1):port(1):dev_name(<=64)" and that of **remote-id** is "user_mac(6):iftype(1):port_name(<=64):vid(2)".

Common Errors

- Basic DHCP Relay functions are not configured.

1.4.6 Configuring DHCP Relay Check Server-ID

Configuration Effect

- After you configure the **ip dhcp relay check server-id**, a DHCP Relay agent will forward DHCP request packets only to the server specified by the **option server-id** command. Otherwise, they are forwarded to all DHCP servers.

Notes

- You need to enable basic DHCP Relay functions.

Configuration Steps

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Verification

Check whether a DHCP Relay agent sends DHCP request packets only to the server specified by the **option server-id** command.

Related Commands

Configuring DHCP Relay Check Server-ID

Command	**ip dhcp relay check server-id**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring DHCP Relay Check Server-ID

Configuration Steps	● Enable DHCP Relay.Omitted. ● Enable **DHCP Relay check server-id** on an interface.
	Hostname# configure terminal Hostname(config)# ip dhcp relay check server-id
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Hostname# show running-config | include check server-id ip dhcp relay check server-id

Common Errors

- Basic DHCP Relay functions are not configured.

1.4.7 Configuring DHCP Client

Configuration Effect

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

Notes

Products support DHCP Client configuration on Ethernet, FR, PPP and HDLC interfaces.

Configuration Steps

Run the **ip address dhcp** command on an interface.

Verification

Check whether the interface obtains an IP address.

Related Commands

Configuring DHCP Client

Command	**ip address dhcp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	● An Ethernet interface can obtain a dynamic IP address through DHCP. ● An interface configured with PPP encapsulation can obtain a dynamic IP address through DHCP. ● An interface configured with FR encapsulation can obtain a dynamic IP address through DHCP. ● An interface configured with HDLC encapsulation can obtain a dynamic IP address through DHCP.

Configuration Example

Configuring DHCP Client

Configuration Steps	● 1: Enable port GigabitEthernet 0/1 with DHCP to obtain an IP address.
	Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ip address dhcp
Verification	● 1: Run the **show running-config** command to display the configuration.
	Hostname#show running-config | begin ip address dhcp ip address dhcp

1.4.8 Defining Fields in Request Messages on Interfaces

Configuration Effect

Enable DHCP client on a device so that you can define option fields in request messages.

Notes

This feature is applicable on Layer 3 ports.

Configuration Steps

Defining the Class-id Field in Request Mesages

- Optional.
- Run the **ip dhcp client class-id** commmad to define the class-id field.

Defining the Client-id Field in Request Mesages

- Optional.
- Run the **ip dhcp client client-id** commmad to define the client-id field.

Defining the Hostname Field in Request Mesages

- Optional.
- Run the **ip dhcp client hostname** commmad to define the hostname field.

Defining the Lease Field in Request Mesages

- Optional.
- Run the i**p dhcp client lease** commmad to define the lease field.

Defining the Option-list Field in Request Mesages

- Optional.
- Run the **ip dhcp client option-list include** commmad to define the option-list field.

Verification

Run the **show running-config** command to check whether the configuration is successful. The device obtains a DHCP request packet and check whether the option field in the packet is customized.

Related Commands

Defining the Class-id Field in Request Mesages

Command	**ip dhcp client class-id** { **ascii** *string* | **hex** *string* }
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Defining the Client-id Field in Request Mesages

Command	**ip dhcp client client-id** { **ascii** *string* | **hex** *string* | **exclude interface-name** }
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Defining the Hostname Field in Request Mesages

Command	**ip dhcp client hostname** *string*
Parameter Description	N/A

Command Mode	Interface configuration mode
Usage Guide	N/A

Defining the Lease Field in Request Mesages

Command	**ip dhcp client lease** *days* [*hours*] [*minutes*]
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Defining the Option-list Field in Request Mesages

Command	**ip dhcp client option-list include** *string*
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ Defining the Class-id Field in Request Mesages

Configuration Steps	1: Define the class-id field as test.
	Hostname(config-if-GigabitEthernet 0/1)#ip dhcp client class-id ascii test
Verification	Run the **show running-config** command to display the configuration.

↘ Defining the Client-id Field in Request Mesages

Configuration Steps	1: Define the client-id field as 0102.0304.0506.
	Hostname(config-if-GigabitEthernet 0/1)#ip dhcp client client-id hex 0102.0304.0506
Verification	Run the **show run** command to display the configuration.

↘ Defining the Hostname Field in Request Mesages

Configuration Steps	1: Define the hostname as Hostname.
	Hostname(config-if-GigabitEthernet 0/1)#ip dhcp client hostname Hostname
Verification	Run the **show running-config** command to display the configuration.

Defining the Lease Field in Request Mesages

Configuration Steps	1: Set the lease time to 1 hour.
	Hostname(config-if-GigabitEthernet 0/1)#ip dhcp client lease 0 1
Verification	Run the **show running-config** command to display the configuration.

Defining the Option-list Field in Request Mesages

Configuration Steps	1: Define the option-list field as 66, 67, 43.
	Hostname(config-if-GigabitEthernet 0/1)#ip dhcp client option-list include 66-67,43
Verification	Run the **show running-config** command to display the configuration.

1.4.9 Releasing and Renewing DHCP Leases

Configuration Effect

After dynamically obtaining IP addresses, DHCP clients release or renews DHCP leases.

Notes

This functionality applies to DHCP clients that obtain IP addresses dynamically. After the interface addresses are released, run the **renew-dhcp** command to recover dynamic addresses or run the **no ip address dhcp** command to start a new request for IP address.

Configuration Steps

Enabling DHCP Clients to Release Dynamic IP Addresses

- Run the **release-dhcp** commmad in privilidge EXEC mode.

Enabling DHCP Clients to Renew Dynamic IP Addresses

- Run the **renew-dhcp** commmad in privilidge EXEC mode.

Verification

Run the **show dhcp lease** command to check whether the configurations take effect.

Related Commands

Enabling DHCP Clients to Release Dynamic IP Addresses

Command	**release-dhcp** *type number*
Parameter Description	N/A
Command Mode	Privilidge EXEC mode
Usage Guide	N/A

Enabling DHCP Clients to Renew Dynamic IP Addresses

Command	**renew-dhcp** *type number*
Parameter Description	N/A
Command Mode	Privilidge EXEC mode
Usage Guide	N/A

Configuration Example

Enabling DHCP Clients to Release Dynamic IP Addresses

Configuration Steps	1: Release the dynamic IP addresses obtained by VLAN 100.
	Hostname# release-dhcp vlan 100
Verification	1: Run the **show dhcp lease** command to display the configuration.

Enabling DHCP Clients to Renew Dynamic IP Addresses

Configuration Steps	1: Renew the dynamic IP addresses obtained by VLAN 100.
	Hostname# renew-dhcp vlan 100
Verification	1: Run the **show dhcp lease** command to display the configuration.

1.4.10 Configuring Class Rules of the DHCP Server

Configuration Effect

After class rules are configured, the DHCP server can assign IP addresses in different network segments to STAs based on the Option 82 information carried by the STAs.

Notes

The configured class rules take effect only after they are associated with corresponding address pools.

Configuration Steps

Configuring CLASS Rules

- Run the **ip dhcp class** command to add class rules.
- Run the **relay agent information** command to enter the Option 82 configuration mode.
- Run the **relay-information hex** command to configure matched Option 82 content.

Associating Class Rules with Address Pools

Run the **class** command to associate class rules.

- Run the **address range** command to configure assigned IP address segments after class rules are matched.

Verification

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

Related Commands

Configuring CLASS Rules

Command	**ip dhcp class** *class-name*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	● Run this command to configure servers. Configure class rules if IP addresses in different network segments need to be assigned based on option information.

Configures address assignment based on class rules.

Command	**ip dhcp use class**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	● Run this command to configure servers.

Enters the Option 82 configuration mode.

Command	**relay agent information**
Parameter Description	N/A

Command Mode	Global class configuration mode
Usage Guide	● Run this command to configure servers and to enter the Option 82 configuration mode.

Configures the Option 82 information matched with class rules.

Command	**relay-information hex**
Parameter Description	N/A
Command Mode	Global class configuration mode
Usage Guide	● Run this command to configure servers and to configure the Option 82 information matched with class rules.

Associating Class Rules with Address Pools

Command	**class** *class-name*
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	● Run this command to configure servers and to associate configured class rules with destination address pools.

Configuring the IP Address Range Matched with a Class Rule

Command	**address range** *start-ip end-ip*
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	● Run this command to configure servers and to configure the range of the IP addresses assigned to a STA when a class rule is matched.

Configuration Example

Configuring Class Rules

Configuration Steps	1. Create a global class rule, for example, test-class.
	Hostname(config)# ip dhcp class test-class 2. Enter the **relay-agent-info** configuration mode. Hostname(config-dhcp-class)# relay agent information 3. Add the Option 82 information sent from a specified port as the matching rule.

	Hostname(config-dhcp-class-relayinfo)# relay-information hex 0104001002010203010020 4. Associate the class rule with an address pool and specify the address network segment. Hostname(config)# ip dhcp pool test-pool Hostname(dhcp-config)# class test-class Hostname(config-dhcp-pool-class)# address range 1.1.1.10 1.1.1.20
Verification	● Run the **show running-config** command to check the configuration.
	Hostname# show running-config ip dhcp class test-class relay agent information relay-information hex 0104001002010203010020 ! ip dhcp pool test-pool class test-class address range 1.1.1.10 1.1.1.20

1.5 Monitoring

Clearing

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

Description	Command
Clears DHCP address binding.	**clear ip dhcp binding** { *address* | *}
Clears DHCP address conflict.	**clear ip dhcp conflict** { *address* | *}
Clears the address assigned by the DHCP server.	**clear ip dhcp history** { * | *mac-address* }
Clears statistics of a DHCP server.	**clear ip dhcp server statistics**
Clears statistics of a DHCP relay.	**clear ip dhcp relay statistics**
Clears statistics of DHCP server performance.	**clear ip dhcp server rate**
Clears information of a DHCP pseudo server.	**clear ip dhcp server detect**

Displaying

Description	Command
Displays DHCP lease.	**show dhcp lease**
Displays DHCP sockets.	**show ip dhcp socket**
Displays assigned IP addresses.	**show ip dhcp binding**
Displays created address pools.	**show ip dhcp pool**

Displays statistics of DHCP Server.	**show ip dhcp server statistics**
Displays statistics of DHCP Relay.	**show ip dhcp relay-statistics**
Displays conflicted addresses.	**show ip dhcp conflict**
Displays DHCP lease history.	**show ip dhcp history**
Displays the address pool ID and address utilization of a DHCP server.	**show ip dhcp identifier**
Displays the DHCP pseudo server.	**show ip dhcp server detect**

1 Configuring DHCP Snooping

1.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP snooping records may serve security applications like IP Source Guard.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

1.2 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 Forged DHCP Packets	Malicious network users may send forged DHCP request packets, for example, DHCP-RELEASE packets.
Guarding Against IP/MAC Spoofing	Malicious network users may send forged IP packets, for example, tampered source address fields of packets.
Preventing Lease of IP Addresses	Network users may lease IP addresses rather than obtaining them from a DHCP server.
Detecting ARP Attacks	Malicious users forge ARP response packets to intercept packets during normal users' communication.

1.2.1 Guarding Against DHCP Service Spoofing

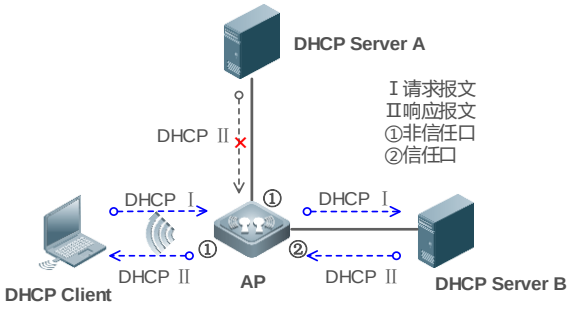
Scenario

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 1-1



Remarks:	AP is the access device. DHCP Server B is the DHCP server under control. DHCP Server A is the uncontrolled DHCP server.

Deployment

- Enable DHCP snooping on AP to realize DHCP packet monitoring.
- Set the port on AP connecting to B as trusted to transfer response packets.
- Set the rest of ports on AP as untrusted to filter response packets.

1.2.2 Guarding Against Forged DHCP Packets

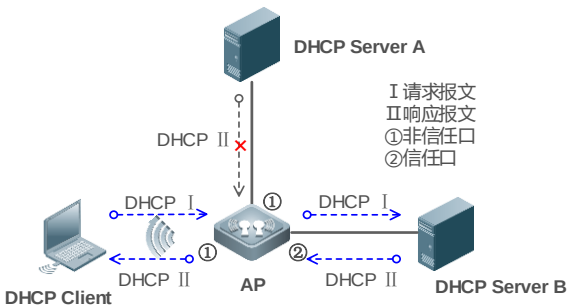
Scenario

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 1-2



Remarks:	AP is the access device. DHCP Server B is the DHCP server under control.

Deployment

- Enable DHCP snooping on AP to realize DHCP monitoring.
- Set the port on AP connecting to B as trusted to transfer response packets.
- Set the rest of ports on AP as untrusted to filter response packets.
- Enable DHCP snooping Source MAC Verification on untrusted ports of AP to filter out illegal packets.

1.2.3 Guarding Against IP/MAC Spoofing

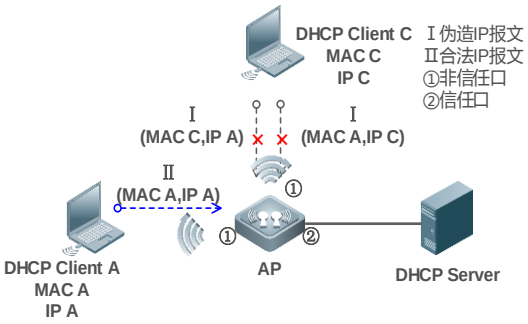
Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP-MAC fields.

For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 1-3



Remarks:	AP is the access device. DHCP Client A and DHCP Client B are user clients. DHCP Server is the DHCP server under control.

Deployment

- Enable DHCP snooping on AP to realize DHCP monitoring.
- Set all downlink ports on the AP as DHCP snooping untrusted.
- Enable IP Source Guard on AP to filter IP packets.
- Enable IP Source Guard in IP-MAC based mode to check the source MAC and IP address fields of IP packets.

1.2.4 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

1.2.5 Detecting ARP Attacks

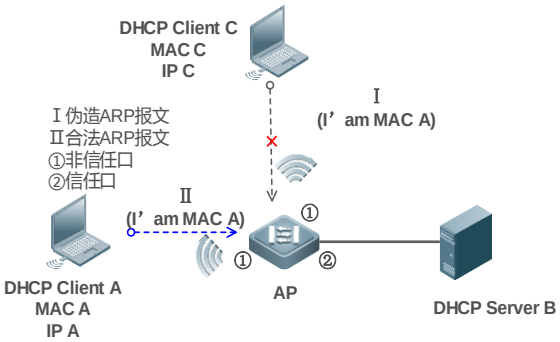
Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP snooping histories.

Figure 1-4



Remarks:	AP is the access device. DHCP Client A and DHCP Client C are user clients. DHCP Server B is the DHCP server under control.

Deployment

- Enable DHCP snooping on AP to realize DHCP monitoring.
- Set all downlink ports on the AP as untrusted.
- Enable IP Source Guard and ARP Check on all the untrusted ports on AP to realize ARP packet filtering.

⚠ All the above security control functions are only effective to DHCP snooping untrusted ports.

1.3 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 the device, all Layer 2 aggregate interfaces are untrusted ports by default. You can specifiy trusted ports. On wireless access points (APs), all the WLAN interfaces are untrusted and cannot be specified as trusted. In fat AP configuration mode, all the layer-2 switching ports and layer-2 encapsulation sub-interfaces are untrusted by default, and can be specified as trusted. In fit AP configuration mode, all the layer-2 switching ports are untrusted by default and can be specified as trusted, and all the layer-2 encapsulation sub-interfaces are trusted and cannot be specified as untrusted. On wireless access controllers (ACs), all WLAN interfaces are untrusted ports and cannot be specified as trusted, and all the switching ports and layer-2 aggregate ports are untrusted ports by default and can be specified as trusted.

DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP snooping packet suppression on its untrusted ports.

VLAN-based DHCP Snooping

DHCP snooping can work on a VLAN basis. By default, when DHCP snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP snooping flexibly.

DHCP Snooping Binding Database

In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP snooping binding database. Combined with ARP detection and ARP check, DHCP snooping controls the reliable assignment of IP addresses for legal clients.

DHCP Snooping Rate Limit

DHCP snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay services of a

network access device like DHCP Relay and DHCP snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

↘ Illegal DHCP Packets

Through DHCP snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP ACK, DHCP NAK 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 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.

1.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

Working Principle

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

↘ Checking Ports

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

↘ Checking Packet Encapsulation and Length

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

Checking Packet Fields and Types

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check whether the restrictive conditions for the type of the packet are met.

Related Configuration

Enabling Global DHCP Snooping

By default, DHCP snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP snooping must be enabled before VLAN-based DHCP snooping is applied.

Configuring VLAN-based DHCP Snooping

By default, when global DHCP snooping is effective, DHCP snooping is effective to all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

Configuring DHCP Snooping Source MAC Verification

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified.

When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP REQUEST packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

1.3.2 Building the Binding Database

DHCP snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

Generating Binding Entries

When a DHCP ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index or a WLAN ID) 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.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Features	⚠ (Mandatory) It is used to enable DHCP Snooping.	
	ip dhcp snooping	Enables DHCP Snooping.
	ip dhcp snooping bootp-bind	Enable DHCP Snooping BOOTP-bind function.
	ip dhcp snooping suppression	Enables DHCP Snooping packet suppression.
	ip dhcp snooping vlan	Enables VLAN-based DHCP Snooping.
	ip dhcp snooping verify mac-address	Configures DHCP Snooping source MAC verification.
	ip dhcp snooping database write-delay	Writes the DHCP Snooping binding database to Flash periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP Snooping binding database to Flash manually.
	renew ip dhcp snooping database	Manually import user records in back up files to the DHCP snooping binding database.
	ip dhcp snooping database	Configure the backup files of 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.
	ip dhcp snooping clear-broadcast-flag	Enables the function of clearing the broadcast flag bit.
Configuring Option82	⚠ (Optional)It is used to optimize the address assignment by DHCP servers.	
	ip dhcp snooping Information option	Adds Option82 functions to DHCP request packets.
	ip dhcp snooping information option format remote-id	Configures the sub-potion **remote-id** of Option82 as a user-defined character string.
	ip dhcp snooping vlan information option format-type circuit-id string	Configures the sub-option **circuit-id** of Option82 as a user-defined character string.

1.4.1 Configuring Basic Features

Configuration Effect

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

Notes

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces, as well as WLAN interfaces. The configuration can be implemented in interface configuration mode and WLAN security configuration mode.

Configuration Steps

↘ Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

↘ Enabling or Disabling VLAN-based DHCP Snooping

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

↘ Configuring DHCP Snooping Trusted Ports

- Mandatory.
- Configure the ports connecting a trusted DHCP server as trusted.

↘ Enabling DHCP Snooping Source MAC Validation

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

↘ Writing the DHCP Snooping Binding Database to Flash Periodically

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- The device does not save information about wireless clients.
- 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 Correlation with ARP

- Optional.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping to Process Relay Requests

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

Enabling DHCP Snooping

- Optional.
- If DHCP Snooping binding entries need to be generated on a routed port, the feature should be enabled on a Layer 3 device.

Enabling DHCP Snooping to Clear the Broadcast Flag Bit

- Optional.
- Unless otherwise noted, the feature should be enabled in large Layer-2 wireless scenarios.

Enabling Fast Aging of DHCP Snooping Migration Entries

- Optional.

Enabling Migration of DHCP Snooping Binding Entries

- Optional.

Enabling DHCP Snooping to generate static ARP Entries

- Optional.

Enabling DHCP Snooping Forwarding in Loose Mode

Optional.

- Unless otherwise noted, the feature should be disabled.

Verification

Configure a client to obtain network configurations through the DHCP protocol.

- Check whether the DHCP Snooping Binding database is generated with entries on the client.

Related Commands

Enabling or Disabling DHCP Snooping

Command	[**no**] **ip dhcp snooping**
Parameter Description	**N/A**
Command	Global configuration mode

Mode	
Usage Guide	After global DHCP Snooping is enabled, you can check DHCP Snooping using the **show ip dhcp snooping** command.

Enable DHCP Snooping BOOTP-bind function.

Command	[**no**] **ip dhcp snooping bootp-bind**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

Configuring VLAN-based DHCP Snooping

Command	[**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Parameter Description	*vlan-rng*: Indicates the range of VLANs *vlan-min*: The minimum VLAN ID *vlan-max*: The maximum VLAN ID
Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable DHCP Snooping on specified VLANs. This feature is available only after global DHCP Snooping is enabled.

Configuring DHCP Snooping Packet Suppression

Command	[**no**] **ip dhcp snooping suppression**
Parameter Description	**N/A**
Command Mode	dot11radio interface configuration mode/WLAN security 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	*time*: Indicates the interval between two times of writing the DHCP Snooping database to the Flash.
Command Mode	Global configuration mode
Usage Guide	Use this command to write the DHCP Snooping database to FLASH document. This can avoid binding information loss which requires re-obtaining IP addresses to resume communication after the device restarts.

Writing the DHCP Snooping Database to Flash Manually

Command	**ip dhcp snooping database write-to-flash**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Use this command to write the dynamic user information in the DHCP Snooping database in FLASH documents in real time. If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored from FLASH documents because of version differences between FLASH documents.

Importing Backep File Storage to the DHCP Snooping Binding Database

Command	**renew ip dhcp snooping database**
Parameter Description	**N/A**
Command 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 Description	**N/A**
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a port connected to a legal DHCP server as a trusted port. The DHCP response packets received by trusted ports are transferred, while those received by untrusted ports are discarded.

Enabling or Disabling BOOTP Support

Command	[**no**] **ip dhcp snooping bootp-bind**
Parameter Description	**N/A**

Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOPT protocol.

Enabling DHCP Snooping to Process Relay Requests

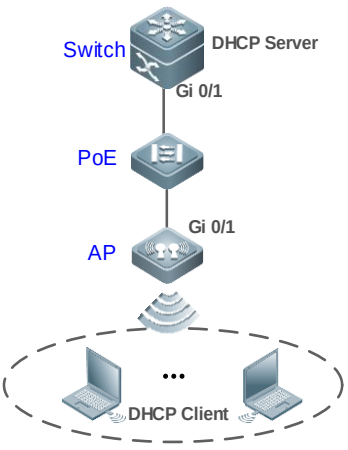
Command	[**no**] **ip dhcp snooping check-giaddr**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet. After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

Enabling DHCP Snooping to Clear the Broadcast Flag Bit

Command	[**no**] **ip dhcp snooping clear-broadcast-flag**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, DHCP Snooping checks the broadcast flag bit for non-DHCP Relay requests. If the flag bit is 1, it clears the flag bit. When receiving responses, DHCP Snooping sets the flag bit to 1 and set Layer-2 and Layer-3 destination addresses as broadcast addresses.

Configuration Example

DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Scenario **Figure 1-5**	

Configuration Steps	● Enable DHCP Snooping on an access device AP. ● Configure the uplink port (port GigabitEthernet 0/1 in this case) as a trusted port.
AP	Hostname# configure terminal Hostname(config)#ip dhcp snooping Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# encapsulation dot1Q 1 Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping trust Hostname(config)# interface Dot11radio 1/0 Hostname(config-if- Dot11radio 1/0)# ip dhcp snooping trust
Verification	Check the configuration on AP. ● Check whether DHCP Snooping is enabled, and whether the configured DHCP Snooping trusted port is uplink. ● Check the DHCP Snooping configuration on AP, and especially whether the trusted port is correct.
AP	Hostname# show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 Hostname# 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) ---------- ------- ---------- Dot11radio 1/0 YES unlimited GigabitEthernet 0/1 YES unlimited Hostname# show ip dhcp snooping binding Total number of bindings: 1 MacAddress IpAddress Lease(sec) Type VLAN Interface ---------- ---------- ---------- ---------- ----- ---------- 0013.2049.9014 192.168.10.25 86207 DHCP-Snooping 1 GigabitEthernet 0/1

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.

1.4.2 Configuring Option82

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Opion82 functions for DHCP Snooping and DHCP Relay are mutually exclusive.

Configuration Steps

- To realize optimization of address allocation, implement the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP Snooping enabled.

Verification

Check whether the DHCP Snooping configuration options are configured successfully.

Related Commands

↘ Adding Option82 to DHCP Request Packets

Command	[**no**] **ip dhcp snooping information option** [**standard-format** | **format**]
Parameter Description	**standard-format**: Indicates a standard format of the Option82 options **format:** Option82 format
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	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Parameter Description	**string** *ASCII-string*: Indicates the content of the extensible format, the Option82 option **remote-id**, is a user-defined character string **hostname**: Indicates the content of the extensible format, the Option82 option **remote-id**, is a host name.
Configuration mode	Global configuration mode
Usage Guide	Use this command to configure the sub-option **remote-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

↘ Configuring Sub-Option circuit -id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter Description	*vlan-id*: Indicates the VLAN where a DHCP request packet is *ascii-string*: Indicates the user-defined string
Configuration mode	Interface configuration mode
Usage Guide	Use this command to configure the sub-option **circuit-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuration Example

Configuring Option82 to DHCP Request Packets

Configuration Steps	● Configuring basic functions of DHCP Snooping. ● Configuring Option82.
AP	Hostname# configure terminal Hostname(config)# ip dhcp snooping information option Hostname(config)# end
Verification	Check the DHCP Snooping configuration.
AP	Hostname# show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : ENABLE DHCP Snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ---------- ------- ---------- GigabitEthernet 0/1 YES unlimited

Common Errors

- N/A

1.5 Monitoring

Clearing

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

Description	Command
Clears the DHCP Snooping binding database.	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id* | **wlan** *wlan-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**
Debugs DHCP Snooping based on MAC addresses.	**debug snooping ipv4 mac-address** *H.H.H*
Disables debugging DHCP Snooping based on MAC addresses.	**no debug snooping ipv4 mac-address** *H.H.H*
Debugs all DHCP Snooping functions.	**debug snooping ipv4 all**
Disables debugging all DHCP Snooping.	**no debug snooping ipv4 all**

1 Configuring DNS

1.1 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

1.2 Applications

N/A

1.3 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.

1.3.1 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.
- Run the **ipv6 host** command to specify the IPv6 address mapped to a domain name.

Configuring a DNS Server

- By default, no DNS server is configured.
- Run the **ip name-server** command to configure a DNS server.

1.4 Configuration

Configuration	Description and Command	
Configuring Static Domain Name Resolution	⚠ Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip host	Configures the IPv4 address mapped to a domain name.
	ipv6 host	Configures the IPv6 address mapped to a domain name.

Configuring Dynamic Domain Name Resolution	⚠ Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip name-server	Configures a DNS server.

1.4.1 Configuring Static Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name on a local device.

Configuration Steps

↘ Enabling Domain Name Resolution

- The domain name resolution function is enabled by default.
- If this function is disabled, static domain name resolution does not take effect.

↘ Configuring the IP Address Mapped to a Domain Name

- (Mandatory) Domain names to be used must be configured with mapped IP addresses.

Verification

- Run the **show running-config** command to check the configuration.
- Run the **show hosts** command to check the mapping between the domain name and the IP address.

Related Commands

↘ Enabling Domain Name Resolution

Command	**ip domain-lookup**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the IPv4 Address Mapped to a Domain Name

Command	**ip host** *host-name ip-address*
Parameter Description	*host-name*: indicates a domain name. *ip-address*: indicates a mapped IPv4 address.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the IPv6 Address Mapped to a Domain Name

Command	**ipv6 host** *host-name ipv6-address*

Parameter Description	*host-name*: indicates a domain name. *ipv6-address*: indicates a mapped IPv6 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Static Domain Name Resolution

Configuration Steps	● Set the IP address of static domain name www.test.com to 192.168.1.1 on a device. ● Set the IP address of static domain name www.testv6.com to 2001::1 on a device.
	Hostname#configure terminal Hostname(config)# ip host www.test.com 192.168.1.1 Hostname(config)# ipv6 host www.testv6.com 2001::1 Hostname(config)# exit
Verification	Run the **show hosts** command to check whether the static domain name entry is configured.
	Hostname#show hosts Name servers are: Host type Address TTL(sec) www.test.com static 192.168.1.1 --- www.testv6.com static 2001::1 ---

1.4.2 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 running-config** command to check the configuration.

Related Commands

Enabling Domain Name Resolution

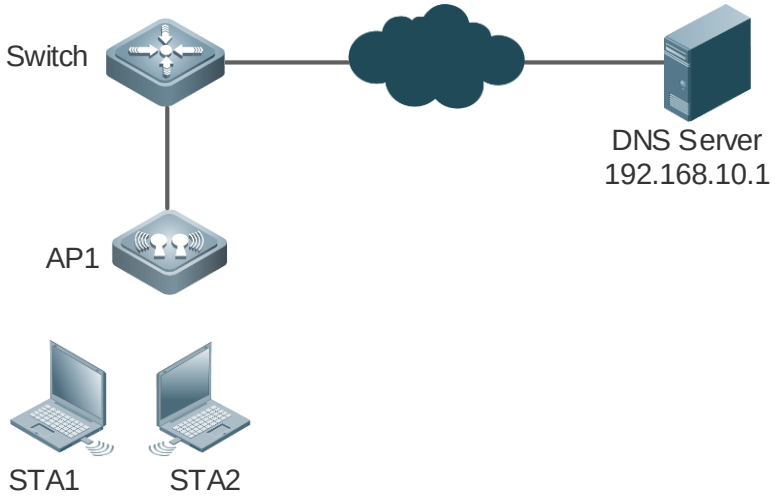
Command	**ip domain-lookup**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a DNS Server

Command	**ip name-server**{ *ip-address* | *ipv6-address* }
Parameter Description	*ip-address*: indicates the IPv4 address of the DNS server. *Ipv6-address*: indicates the IPv6 address of the DNS server.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Dynamic Domain Name Resolution

Scenario Figure 1-1	
	Device resolves the domain name through the DNS server (192.168.10.1) on the network.
Configuration Steps	Set the IPv4 address of the DNS server to 192.168.10.1 on the device. Set the IPv4 address of the DNS server to 2001::1 on the device.
	Hostname# configure terminal Hostname(config)# ip name-server 192.168.10.1 Hostname(config)# ip name-server 2001::1 Hostname(config)# exit

Verification	Run the **show hosts** command to check whether the DNS server is specified.
	Hostname# show hosts Name servers are: 192.168.10.1 static 2001::1 static Host type Address TTL(sec)

1.5 Monitoring

Clearing

⚠ Running the **clear** command during device operation may cause data loss or even interrupt services.

Description	Command
Clears the dynamic host name cache table.	**clear host** [*host-name*]

Displaying

Description	Command
Displays DNS parameters.	**show hosts** [*host-name*]

1 Configuring DNS SNOOPING

1.1 Overview

DNS SNOOPING snoops the domain name server (DNS) packets exchanged between clients and servers to record the mapping table entries of domain names and IP addresses. It can also filter invalid DNS packets, including request packets from clients and response packets from servers.

DNS SNOOPING supports the following function:

Settings of authentication-free uniform resource locators (URLs), that is, domain name-based direct-through addresses.

Protocols and Standards

- RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

1.2 Applications

N/A

1.3 Features

Basic Concepts

Authentication-free App

Unauthenticated clients can access authentication-free Apps, such as WeChat and Sina Weibo.

Authentication-free URL

Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, clients are allowed to access specific URLs without authentication.

CWMP

CPE WAN Management Protocol (CWMP) is a technical standard initiated by Digital Subscriber's Line (DSL) forum and numbered TR-069. Therefore, CWMP is also known as TR-069 protocol. It provides the universal framework, message specification, method and data model for managing and configuring home network devices in next-generation networks.

The implementation of TR-069 protocol is complex. For App authentication, TR-069 provides the network channel for communication between the AC and the MCP server.

Overview

Feature	Description
Authentication-free URL	Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, clients are allowed to access specific URLs without authentication.

1.3.1 Authentication-free URL

After the authentication-free URL function is enabled on the AC, unauthenticated clients are allowed to access specific URLs.

Working Principle

Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, if the AC determines that traffic of an unauthenticated client contains the URL characteristics, the AC allows the traffic to pass and the client can access the specific URL without authentication.

1.4 Configuration

Configuration	Description and Command	
Configuring Authentication-free URL	⚠ (Mandatory) It is used to configure authentication-free Apps in global configuration mode.	
	free-url	Configures the authentication-free URL. At present, only WeChat, Sina App, certain iPhone Apps, and designated URLs are supported.
	ip dns snooping enable	Enables DNS SNOOPING.

1.4.1 Configuring Authentication-free URL

Configuration Effect

- Allow unauthenticated clients to access the configured authentication-free URL directly.

Notes

- The authentication-free URL takes effect only after the Web-based authentication function is enabled.

Configuration Steps

↘ Enabling DNS SNOOPING

- Mandatory.
- Enable DNS SNOOPING on the device.

Command	**ip dns snooping enable**
Parameter Description	N/A
Defaults	DNS snooping is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Run this command to enable DNS SNOOPING.

Configuring Authentication-free URL

- Mandatory.
- Configure an authentication-free URL on the AC.

Command	**free-url** { **weixin** | **sina** | **iphone** | **url** *url* }
Parameter Description	**weixin**: Indicates WeChat. **sina**: Indicates a Sina App. **iphone**: Indicates an iPhone App. *url*: Indicates a designated URL.
Defaults	No authentication-free URL is configured by default.
Command Mode	Global configuration mode
Usage Guide	You can configure multiple authentication-free URLs.

Verification

- Run the **show free-url** command to check the configuration status.
- Check whether unauthenticated clients can access the authentication-free URLs directly when the Web-based authentication function is enabled on the AC.

Configuration Example

Configuring WeChat as Authentication-free URL on AC

Configuration Steps	• Enter the global configuration mode. • Configure WeChat as an authentication-free URL.
Device	Hostname#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#ip dns snooping enable Hostname(config)# free-url weixin Hostname(config)# free-url *.baidu.com Hostname(config)#exit
Verification	Run the **show free-url** command to check the authentication-free URL information.
Device	Hostname# show free-url Total number of domain name : 4 Total number of ip address : 11

```
======================== free-url domain name table ========================
Host                    type      Interface                          Vlan      Wlan
*.qpic.cn               weixin    all                                all       all
*.weixin.qq.com         weixin    all                                all       all
weixin.qq.com           weixin    all                                all       all
*.baidu.com             url       all                                all       1
============================================================================


========================== free-url ip table ==============================
Host                    type      Address                            TTL(sec)
*.weixin.qq.com         weixin    61.151.224.41                      2118
                                  140.207.135.125                    2118
                                  140.207.54.47                      2118
*.qpic.cn               weixin    140.206.160.234                    2118
                                  183.61.49.180                      151
                                  101.226.129.204                    554
                                  14.17.52.136                       16
weixin.qq.com           weixin    14.17.42.45                        800
*.baidu.com             url       115.239.210.246                    19
                                  115.239.211.235                    2286
                                  115.239.210.14                     284
============================================================================
```

1.5 Monitoring

Clearing

Displaying

Description	Command
Displays authentication-free URLs.	**show free-url**
Clears authentication-free URLs.	**clear free-url**
Displays the statistics on DNS packets.	**show dns snooping statistics**

1 Configuring IPv6 Basics

1.1 Overview

As the Internet develops rapidly and IPv4 address space is becoming exhausted, IPv4 limitations become more and more obvious. At present, many researches and practices on Internet Protocol Next Generation (IPng) have been conducted. The IPng working group of the Internet Engineering Task Force (IETF) has formulated an IPng protocol named IP Version 6 (IPv6), which is described in RFC 2460.

Main Features

↘ Larger Address Space

Compared with 32 bits in an IPv4 address, the length of an IPv6 address is extended to 128 bits. Therefore, the address space has approximately 2^{128} addresses. IPv6 adopts a hierarchical address allocation mode to support address allocation of multiple subnets from the Internet core network to intranet subnet.

↘ Simpler Packet Header Format

Since the design principle of the IPv6 packet header is to minimize the overhead of the packet header, some non-key fields and optional fields are removed from the packet header to the extended packet header. Therefore, although the length of an IPv6 address is four times of that of an IPv4 address, the IPv6 packet header is only two times of the IPv4 packet header. The IPv6 packet header makes device forwarding more efficient. For example, with no checksum in the IPv6 packet header, the IPv6 device does not need to process fragments (fragmentation is completed by the initiator).

↘ Efficient Hierarchical Addressing and Routing Structure

IPv6 uses a convergence mechanism and defines a flexible hierarchical addressing and routing structure. Multiple networks at the same layer are represented as a uniform network prefix on the upstream device, greatly reducing routing entries maintained by the device and routing and storage overheads of the device.

↘ Easy Management: Plug and Play (PnP)

IPv6 provides automatic discovery and auto-configuration functions to simplify management and maintenance of network nodes. For example, Neighbor Discovery (ND), MTU Discovery, Router Advertisement (RA), Router Solicitation (RS), and auto-configuration technologies provide related services for PnP. Particularly, IPv6 offers two types of auto-configuration: stateful auto-configuration and stateless auto-configuration. In IPv4, Dynamic Host Configuration Protocol (DHCP) realizes auto-configuration of the host IP address and related parameters. IPv6 inherits this auto-configuration service from IPv4 and called it stateful auto-configuration (see DHCPv6). Besides, IPv6 also offers the stateless auto-configuration service. During stateless auto-configuration, a host automatically obtains the local address of the link, address prefix of the local device, and other related configurations.

↘ Security

As an optional extension protocol of IPv4, Internet Protocol Security (IPSec) is a part of IPv6 to provide security for IPv6 packets. IPv6 provides two mechanisms: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH provides data integrity and authenticates IP packet sources to ensure that the packets originate from the nodes identified by the source addresses. ESP provides data encryption to realize end-to-end encryption.

↘ Better QoS Support

A new field in the IPv6 packet header defines how to identify and process data streams. The Flow Label field in the IPv6 packet header is used to authenticate a data flow. Using this field, IPv6 allows users to propose requirements on the communication quality. , A device can identify all packets belonging to a specific data stream based on this field and process these packets according to user requirements.

↘ New Protocol for Neighboring Node Interaction

IPv6 Neighbor Discovery Protocol (NDP) uses a series of Internet Control Message Protocol Version 6 (ICMPv6) packets to implement interactive management of neighboring nodes (nodes on the same link). IPv6 uses NDP packets and efficient multicast/unicast ND packets instead of broadcast-based Address Resolution Protocol (ARP) and Control Message Protocol Version 4 (ICMPv4) router discovery packets.

↘ Extensibility

With strong extensibility, IPv6 features can be added to the extended packet header following the IPv6 packet header. Unlike IPv4, the IPv6 packet header can support at most 40 bytes of options. For an IPv6 packet, the length of the extended packet header is restricted only by the maximum number of bytes in the packet.

Protocols and Standards

- RFC 4291 - IPVersion6AddressingArchitecture
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 - IPv6 Stateless Address Auto-configuration
- RFC 5059 - Deprecation of Type 0 Routing Headers in IPv6

1.2 Applications

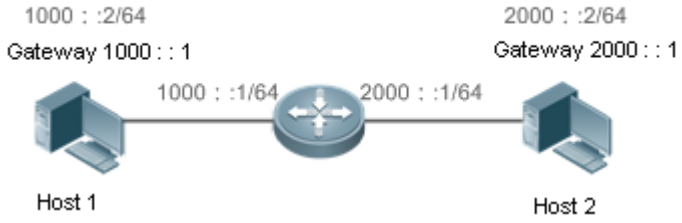
Application	Description
Communication Based on IPv6 Addresses	Two PCs communicate with each other using IPv6 addresses.

1.2.1 Communication Based on IPv6 Addresses

Scenario

As shown in Figure 1-1, Host 1 and Host 2 communicate with each other using IPv6 addresses.

Figure 1-1



Deployment

Hosts can use the stateless address auto-configuration or DHCPv6 address assignment mode. After addresses are configured, hosts can communicate with each other using IPv6 addresses.

1.3 Features

Overview

Feature	Description
IPv6 Address Format	The IPv6 address format makes IPv6 have a larger address space and flexible representation approach.
IPv6 Address Type	IPv6 identifies network applications based on addresses.
IPv6 Packet Header Format	IPv6 simplifies the fixed and extended packet headers to improve the data packet processing and forwarding efficiency of the device.
IPv6 PMTUD	A host dynamically discovers and adjusts the MTU size on the data Tx path, saving router resources and improving IPv6 network efficiency.
IPv6 Neighbor Discovery	ND functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and redirection.
IPv6 Source Routing	Specifies the intermediate nodes that a packet passes through along the path to the destination address. It is similar to the IPv4 loose source routing option and loose record routing option.
Restricting the Sending Rate of ICMPv6 Error Messages	Prevents DoS attacks.
IPv6 Hop Limit	Prevents useless unicast packets from being unlimitedly transmitted on the network and wasting network bandwidth.
Configuring the Device Enabled with IPv6 ND to Allocate Different Prefixes to Different Users	Allocates different IPv6 prefixes to different users.

Feature	Description
Enabling ND Packet Rate Statistics Collection	Counts the number of ND packets sent and received on all IPv6 interfaces, and their corresponding rates.

1.3.1 IPv6 Address Format

An IPv6 address is represented in the X:X:X:X:X:X:X:X format, where X is a 4-digit hexadecimal integer (16 bits). Each address consists of 8 integers, with a total of 128 bits (each integer contains 4 hexadecimal digits and each digit contains four bits). The following are three valid IPv6 addresses:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

These integers are hexadecimal, where A to F represent 10 to 15. Each integer in the address must be represented, except the leading zeros in each integer. If an IPv6 address contains a string of zeros (as shown in the second and third examples above), a double colon (::) can be used to represent these zeros. That is, 800:0:0:0:0:0:0:1 can be represented as 800::1.

A double colon indicates that this address can be extended to a complete 128-bit address. In this approach, only when the 16-bit integers are all 0s, can they can be replaced with a double colon. A double colon can exist once in an IPv6 address.

In IPv4/IPv6 mixed environment, an address has a mixed representation. In an IPv6 address, the least significant 32 bits can be used to represent an IPv4 address. This IPv6 address can be represented in a mixed manner, that is, X:X:X:X:X:X:d.d.d.d, where X is a hexadecimal integer and d is a 8-bit decimal integer. For example, 0:0:0:0:0:0:192.168.20.1 is a valid IPv6 address. It can be abbreviated to :::192.168.20.1. Typical applications are IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. If the first 96 bits are 0 in an IPv4-compatible IPv6 address, this address can be represented as ::A.B.C.D, e.g., ::1.1.1.1. IPv4-compatible addresses have been abolished at present. IPv4-mapped IPv6 addresses are represented as ::FFFF:A.B.C.D to represent IPv4 addresses as IPv6 addresses. For example, IPv4 address 1.1.1.1 mapped to an IPv6 address is represented as ::FFFF:1.1.1.1.

Since an IPv6 address is divided into two parts: subnet prefix and interface ID, it can be represented as an address with an additional value according to an address allocation method like Classless Inter-Domain Routing (CIDR). The additional value indicates how many bits (subnet prefix) in the address represent the network part. That is, the IPv6 node address contains the prefix length. The prefix length is separated from the IPv6 address by a slash. For example, in 12AB::CD30:0:0:0:0/60, the prefix length used for routing is 60 bits.

Related Configuration

↘ Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure an IPv6 address on an interface.
- After configuration, a host can communicate with others using the configured IPv6 address based on DAD.

1.3.2 IPv6 Address Type

RFC 4291 defines three types of IPv6 addresses:

- Unicast address: ID of a single interface. Packets destined to a unicast address are sent to the interface identified by this address.
- Multicast address: ID of an interface group (the interfaces generally belong to different nodes). Packets destined to a multicast address are sent to all interfaces included in this address.
- Anycast address: ID of an interface group. Packets destined to an anycast address are sent to one interface included in this address (the nearest interface according to the routing protocol).

⚠ IPv6 does not define broadcast addresses.

These three types of addresses are described as follows:

↘ Unicast Addresses

Unicast addresses fall into five types: unspecified address, loopback address, link-local address, site-local address, and global unicast address. At present, site-local addresses have been abolished. Except unspecified, loopback, and link-local addresses, all other addresses are global unicast addresses.

- Unspecified address

The unspecified address is 0:0:0:0:0:0:0:0, which is usually abbreviated to ::. It has two general purposes:

1. If a host has no unicast address when started, it uses the unspecified address as the source address to send an RS packet to obtain prefix information from the gateway and thereby generate a unicast address.
2. When an IPv6 address is configured for a host, the device detects whether the address conflicts with addresses of other hosts in the same network segment and uses the unspecified address as the source address to send a Neighbor Solicitation (NS) packet (similar to a free ARP packet).

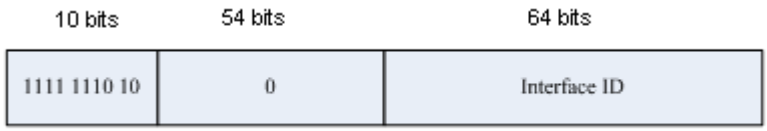
- Loopback address

The loopback address is 0:0:0:0:0:0:0:1, which is usually abbreviated to ::1. Similar to IPv4 address 127.0.0.1, the loopback address is generally used by a node to send itself packets.

- Link-local address

The format of a link-local address is as follows:

Figure 1-2

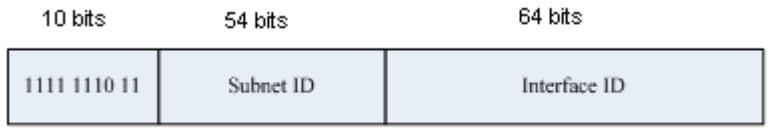


The link-local address is used on a single network link to assign IDs to hosts. The address identified by the first 10 bits in the prefix is the link-local address. A device never forwards packets in which the source or destination address contains the link-local address. The intermediate 54 bits in the address are all 0s. The last 64 bits represent the interface ID, which allows a single network to connect 2^{64}-1 hosts.

- Site-local address

The format of a site-local address is as follows:

Figure 1-3

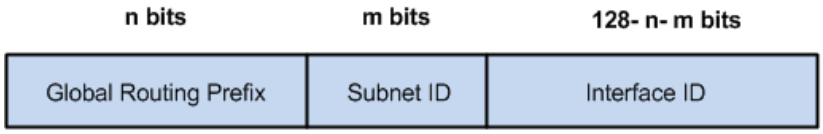


A site-local address is used to transmit data within a site. A device never forwards packets in which the source or destination address contains the site-local address to the Internet. That is, these packets can be forwarded only within the site. A site can be assumed as an enterprise's local area network (LAN). Such addresses are similar to IPv4 private addresses such as 192.168.0.0/16. RFC 3879 has abolished site-local addresses. New addresses do not support the first 10 bits as the prefix and are all regarded as global unicast addresses. Existing addresses can continue to use this prefix.

- Global unicast address

The format of a global unicast address is as follows:

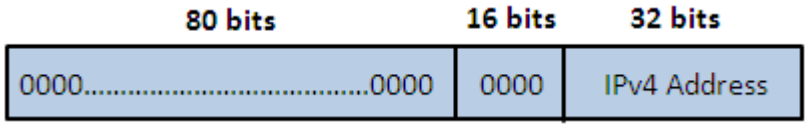
Figure 1-4



Among global unicast addresses, there is a type of IPv4-embedded IPv6 addresses, including IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. They are used for interconnection between IPv4 nodes and IPv6 nodes.

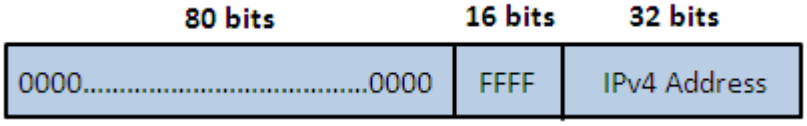
The format of an IPv4-compatible IPv6 address is as follows:

Figure 1-5



The format of an IPv4-mapped IPv6 address is as follows:

Figure 1-6



IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. At present, IPv4-compatible IPv6 addresses have been abolished. IPv4-mapped IPv6 addresses are used by IPv6 nodes to access IPv4-only nodes. For example, if the IPv6 application on an IPv4/IPv6 host requests to resolve the name of an IPv4-only host, the name server dynamically generates an IPv4-mapped IPv6 address and returns it to the IPv6 application.

Multicast Addresses

The format of an IPv6 multicast address is as follows:

```
|    8     |  4 |  4 |                   112 bits                   |
+--------+----+----+----------------------------------------------+
|11111111|flgs|scop|                    group ID                    |
+--------+----+----+----------------------------------------------+
```

The first byte in the address is all 1s, representing a multicast address.

- Flag field

The flag field consists of four bits. Only the fourth bit is specified to indicate whether this address is a known multicast address assigned by the Internet Assigned Numbers Authority (IANA) or a temporary multicast address in a certain scenario. If the flag bit is 0, this address is a known multicast address. If the flag bit is 1, this address is a temporary multicast address. The remaining three flag bits are reserved for future use.

- Scope field

The scope field consists of four bits to indicate the multicast range. That is, a multicast group includes the local node, local link, local site, and any node in the IPv6 global address space.

- Group ID field

The group ID consists of 112 bits to identify a multicast group. A multicast ID can represent different groups based on the flag and scope fields.

IPv6 multicast addresses are prefixed with FF00::/8. One IPv6 multicast address usually identifies interfaces on a series of different nodes. After a packet is sent to a multicast address, the packet is then forwarded to the interfaces on each node identified by this multicast address. For a node (host or device), you must add the following multicast addresses:

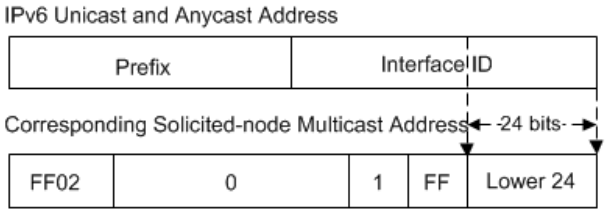
1. Multicast address for all nodes on the local link, that is, FF02::1
2. Solicited-node multicast address, prefixed with FF02:0:0:0:0:1:FF00:0000/104

If the node is a device, it also has to be added to the multicast address of all devices on the local link, that is, FF02::2.

The solicited-node multicast address corresponds to the IPv6 unicast and anycast address. You must add a corresponding solicited-node multicast address for each configured unicast and anycast address of an IPv6 node. The solicited-node multicast address is prefixed with FF02:0:0:0:0:1:FF00:0000/104. The remaining 24 bits are composed of the least significant 24 bits of the unicast or anycast address. For example, if the unicast address is FE80::2AA:FF:FE21:1234, the solicited-node multicast address is FF02::1:FF21:1234.

The solicited-node multicast address is usually used in NS packets. Its address format is as follows:

Figure 1-7



Anycast Addresses

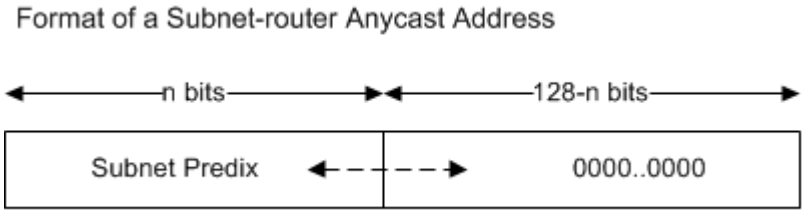
Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node in the anycast address receives data packets while all nodes included in the multicast address receive data packets. Since anycast addresses are allocated to the normal IPv6 unicast address space, they have the same formats with unicast addresses. Every member in an anycast address must be configured explicitly for easier recognition.

Anycast addresses can be allocated only to devices and cannot be used as source addresses of packets.

RFC 2373 redefines an anycast address called subnet-router anycast address. Figure 1-8 shows the format of a subnet-router anycast address. Such an address consists of the subnet prefix and a series of 0s (interface ID).

The subnet prefix identifies a specified link (subnet). Packets destined to the subnet-router anycast address will be forwarded to a device on this subnet. A subnet-router anycast address is usually used by the application on a node to communicate with a device on a remote subnet.

Figure 1-8



Related Configuration

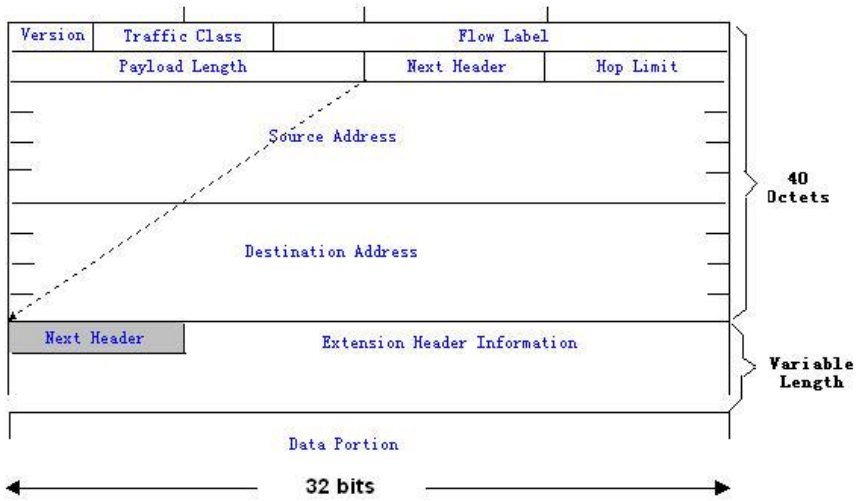
Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure the IPv6 unicast address and anycast address of an interface.
- After an interface goes up, it will automatically join the corresponding multicast group.

1.3.3 IPv6 Packet Header Format

Figure 1-9 shows the format of the IPv6 packet header.

Figure 1-9



The IPv4 packet header is in unit of four bytes. The IPv6 packet header consists of 40 bytes, in unit of eight bytes. The IPv6 packet header has the following fields:

- Version

This field consists of 4 bits. In an IPv6 address, this field must be 6.

- Traffic Class

This field consists of 8 bits. This field indicates the service provided by this packet, similar to the TOS field in an IPv4 address.

- Flow Label

This field consists of 20 bits to identify packets belonging to the same service flow. One node can act as the Tx source of multiple service flows. The flow label and source address uniquely identify one service flow.

- Payload Length

This field consists of 16 bits, including the packet payload length and the length of IPv6 extended options (if available). That is, it includes the IPv6 packet length except the IPv6 packet header.

- Next Header

This field indicates the protocol type in the header field following the IPv6 packet header. Similar to the Protocol field in the IPv4 address header, the Next Header field is used to indicate whether the upper layer uses TCP or UDP. It can also be used to indicate existence of the IPv6 extension header.

- Hop Limit

This field consists of 8 bits. Every time a device forwards a packet, the field value reduced by 1. If the field value reaches 0, this packet will be discarded. It is similar to the Lifetime field in the IPv4 packet header.

- Source Address

This field consists of 128 bits and indicates the sender address in an IPv6 packet.

- Destination Address

This field consists of 128 bits and indicates the receiver address in an IPv6 packet.

At present, IPv6 defines the following extension headers:

- Hop-By-Hop Options

This extension header must follow the IPv6 packet header. It consists of option data to be checked on each node along the path.

- Routing Options (Type 0 routing header)

This extension header indicates the nodes that a packet passes through from the source address to the destination address. It consists of the address list of the passerby nodes. The initial destination address in the IPv6 packet header is the first address among the addresses in the routing header, but not the final destination address of the packet. After the node corresponding to the destination address in the IPv6 packet header receives a packet, it processes the IPv6 packet header and routing header, and sends the packet to the second address, the third address, and so on in the routing header list till the packet reaches the final destination address.

- Fragment

The source node uses this extension header to fragment the packets of which the length exceeds the path MTU (PMTU).

- Destination Options

This extension header replaces the option fields of IPv4. At present, the Destination Options field can only be filled with integral multiples of 64 bits (eight bytes) if required. This extension header can be used to carry information to be checked by the destination node.

- Upper-layer header

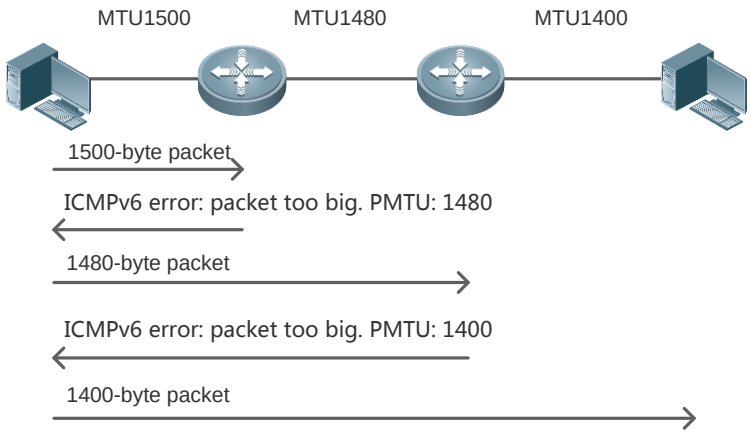
This extension header indicates the protocol used at the upper layer, such as TCP (6) and UDP (17).

Another two extension headers AH and ESP will be described in the *Configuring IPSec*.

1.3.4 IPv6 PMTUD

Similar to IPv4 Path MTU Discovery (PMTUD), IPv6 PMTUD allows a host to dynamically discover and adjust the MTU size on the data Tx path. If the length of a data packet to be sent by a host is greater than the PMTU, the host performs packet fragmentation on its own. In this manner, the IPv6 device does not need to perform fragmentation, saving device resources and improving the IPv6 network efficiency.

Figure 1-10



As shown in Figure 1-10, if the length of a packet to be sent by the host is greater than the PMTU, the router discards this packet and sends an ICMPv6 Packet Too Big message containing its PMTU to the host. The host then fragments the packet based on the new PMTU. In this manner, the router does not need to perform fragmentation, saving router resources and improving the IPv6 network efficiency.

Related Configuration

Configuring the IPv6 MTU of an Interface

- The default IPv6 MTU is 1500 on an Ethernet interface.
- Run the **ipv6 mtu** command to modify the IPv6 MTU of an interface.

Configuring a Static Path MTU

- Run the **ipv6 path-mtu** command to configure a static path MTU.

Configuring the Aging Time for a Dynamic Path MTU

- The default aging time is 10 minutes.
- Run the **ipv6 path-mtu age** command to configure the aging time of the dynamic path MTU.

1.3.5 IPv6 Neighbor Discovery

NDP is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, NUD, DAD, and redirection. NDP defines five ICMP packets: RS (ICMP type: 133), RA (ICMP type: 134), NS (similar to ARP request, ICMP type: 135), NA (similar to ARP reply, ICMP type: 136), ICMP Redirect (ICMP type: 137).

All the above ICMP packets carry one or multiple options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: Source Link-Layer Address Option, Type=1; Target Link-Layer Address Option, Type=2; Prefix Information Option, Type=3; Redirection Header Option, Type=4; MTU Option, Type=5.

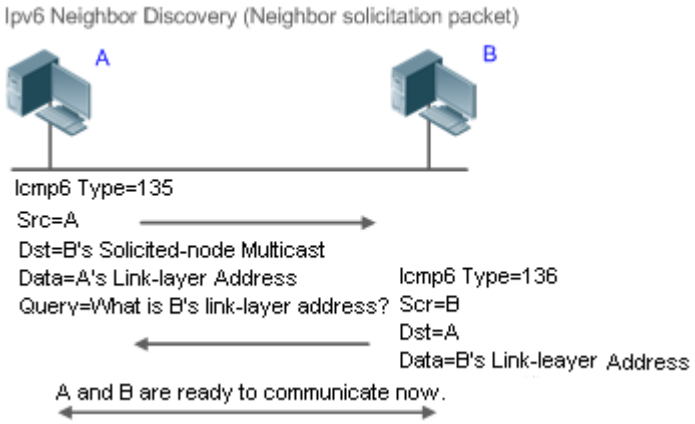
Address Resolution

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer end by sending it an NS packet. In this packet, the destination address is the solicited-node multicast address

corresponding to the IPv6 address of the destination node. This packet also contains the link-layer address of the source node. After receiving this NS packet, the peer end replies with an NA packet in which the destination address is the source address of the NS packet, that is, the link-layer address of the solicited node. After receiving this NA packet, the source node can communicate with the destination node.

Figure 1-11 shows the address resolution process.

Figure 1-11



NUD

If the reachable time of a neighbor has elapsed but an IPv6 unicast packet needs to be sent to it, the device performs NUD.

While performing NUD, the device can continue to forward IPv6 packets to the neighbor.

DAD

To know whether the IPv6 address configured for a host is unique, the device needs to perform DAD by sending an NS packet in which the source IPv6 address is the unspecified address.

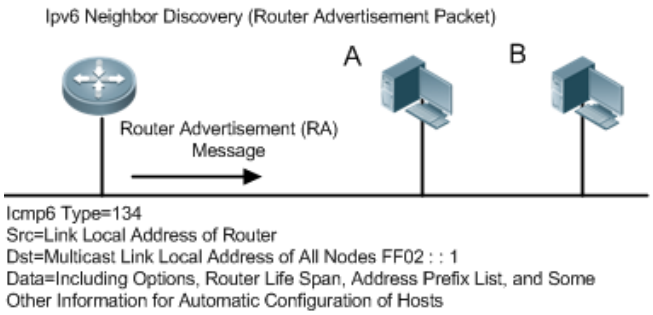
If a device detects an address conflict, this address is set to the duplicate status so that the device cannot receive IPv6 packets with this address being the destination address. Meanwhile, the device also starts a timer for this duplicate address to periodically perform DAD. If no address conflict is detected in re-detection, this address can be properly used.

Router, Prefix, and Parameter Discovery

A device periodically sends RA packets to all local nodes on the link.

Figure 1-12 shows the RA packet sending process.

Figure 1-12



An RA packet usually contains the following content:

- One or multiple IPv6 address prefixes (used for on-link determination or stateless address auto-configuration)
- Validity of the IPv6 address prefix
- Host auto-configuration method (stateful or stateless)
- Default device information (whether the device acts as the default device; if yes, the interval for acting as the default device is also included.)
- Other information provided for host configuration, such as hop limit, MTU, and NS retransmission interval
- Route priority

RA packets can also be used as replies to the RS packets sent by a host. Using RS packets, a host can obtain the auto-configured information immediately after started rather than wait for the RA packets sent by the device. If no unicast address is configured for a newly started host, the host includes the unspecified address (0:0:0:0:0:0:0:0) as the source address in the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all local routing devices (FF02::2) as the destination address in the RS packet. As an reply to the RS packet, the RA packet uses the source address of the RS packet as the destination address (if the source address is the unspecified address, it uses the multicast address of all local nodes (FF02::1).

In an RA packet, the following parameters can be configured:

- Ra-interval: indicates the interval for sending the RA packet.
- Ra-lifetime: indicates the lifetime of a router, that is, whether the device acts as the default router on the local link and the interval for acting as the default router.
- Prefix: indicates the prefix of an IPv6 address on the local link. It is used for on-link determination or stateless address auto-configuration, including other parameter configurations related to the prefix.
- Ns-interval: indicates the NS packet retransmission interval.
- Reachabletime: indicates the period when the device regards a neighbor reachable after detecting a Confirm Neighbor Reachability event.
- Ra-hoplimit: indicates the number of hops of an RA packet, used to set the hop limit for a host to send a unicast packet.
- Ra-mtu: indicates the MTU of an RA packet.

- Managed-config-flag: indicates whether a host receiving this RA packet obtains the address through stateful auto-configuration.
- Other-config-flag: indicates whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

Configure the preceding parameters when configuring IPv6 interface attributes.

- RDNSS and DNSSL options: Provide IPv6 terminals with the address of the DNS recursive query server and a search list of DNS domain names.

Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends the ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time.

Maximum Number of Unresolved ND Entries

- You can configure the maximum number of unresolved ND entries to prevent malicious scanning network segments from generating a large number of unresolved ND entries and occupying excessive memory space.

Maximum Number of ND Options

- You can configure the maximum number of ND options to prevent forged ND packets from carrying unlimited ND options and occupying excessive CPU space on the device.

Maximum Number of Neighbor Learning Entries on an Interface

- You can configure the maximum number of neighbor learning entries on an interface to prevent neighbor learning attacks from occupying ND entries and memory space of the device and affecting forwarding efficiency of the device.

Related Configuration

Enabling IPv6 Redirection

- By default, ICMPv6 Redirect packets can be sent on IPv6 interfaces.
- Run the **no ipv6 redirects** command in interface configuration mode to prohibit an interface from sending Redirect packets.

Configuring IPv6 DAD

- By default, an interface sends one NS packet to perform IPv6 DAD.
- Run the **ipv6 nd dad attempts** *value* command in interface configuration mode to configure the number of NS packets consecutively sent by DAD. Value 0 indicates disabling DAD for IPv6 addresses on this interface.
- Run the **no ipv6 nd dad attempts** command to restore the default configuration.
- By default, the device performs DAD on duplicate IPv6 addresses every 60 seconds.
- Run the **ipv6 nd dad retry** value command in global configuration mode to configure the DAD interval. Value 0 indicates disabling DAD for the device.

- Run the **no ipv6 nd dad retry** command to restore the default configuration.

Configuring the Reachable Time of a Neighbor

- The default reachable time of an IPv6 neighbor is 30s.
- Run the **ipv6 nd reachable-time** *milliseconds* command in interface configuration mode to modify the reachable time of a neighbor.

Configuring the Stale Time of a Neighbor

- The default stale time of an IPv6 neighbor is 1 hour. After the time elapses, the device performs NUD.
- Run the **ipv6 nd stale-time** *seconds* command in interface configuration mode to modify the stale time of a neighbor.

Configuring Prefix Information

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.
- Run the **ipv6 nd prefix** command in interface configuration mode to add or delete prefixes and prefix parameters that can be advertised.

Enabling/disabling RA Suppression

- By default, an IPv6 interface does not send RA packets.
- Run the **no ipv6 nd suppress-ra** command in interface configuration mode to disable RA suppression.

Configuring the Maximum Number of Unresolved ND Entries

- The default value is 0, indicating no restriction. It is only restricted to the ND entry capacity supported by the device.
- Run the **ipv6 nd unresolved** *number* command in global configuration mode to restrict the number of unresolved neighbors. After the entries exceed this restriction, the device does not actively resolve subsequent packets.

Configuring the Maximum Number of ND Options

- Run the **ipv6 nd max-opt** *value* command in global configuration mode to restrict the number of ND options to be processed. The default value is 10.

Configuring the Maximum Number of ND Entries Learned on an Interface

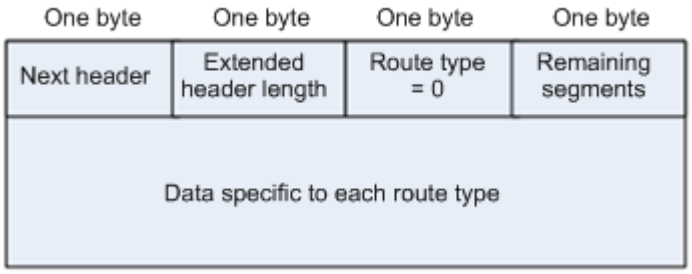
- Run the **ipv6 nd cache interface-limit** *value* command in interface configuration mode to restrict the number of neighbors learned on an interface. The default value is 0, indicating no restriction.

1.3.6 IPv6 Source Routing

Working Principle

Similar to the IPv4 loose source routing and loose record routing options, the IPv6 routing header is used to specify the intermediate nodes that the packet passes through along the path to the destination address. It uses the following format:

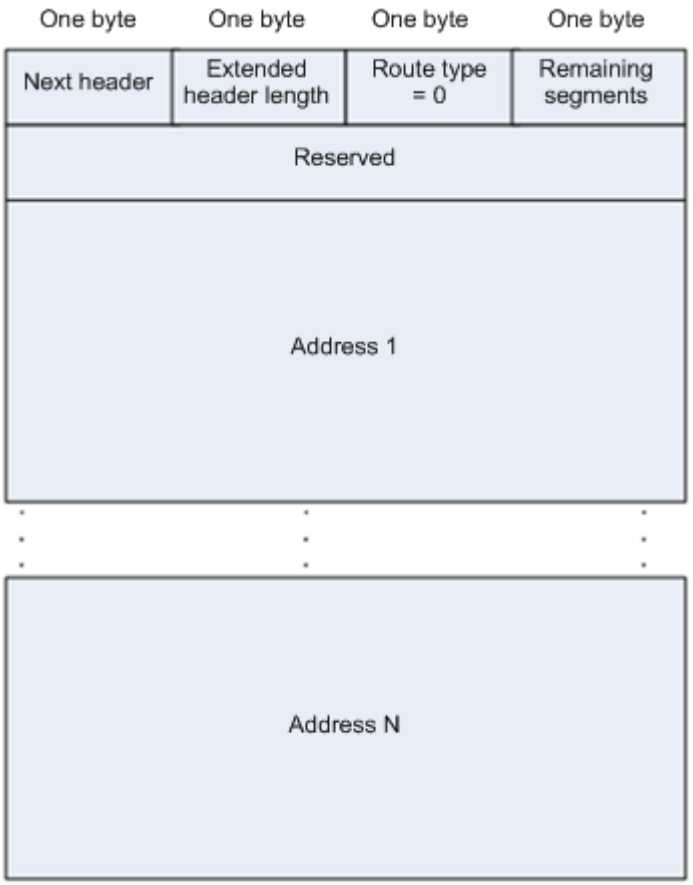
Figure 1-13



The Segments Left field is used to indicate how many intermediate nodes are specified in the routing header for the packet to pass through from the current node to the final destination address.

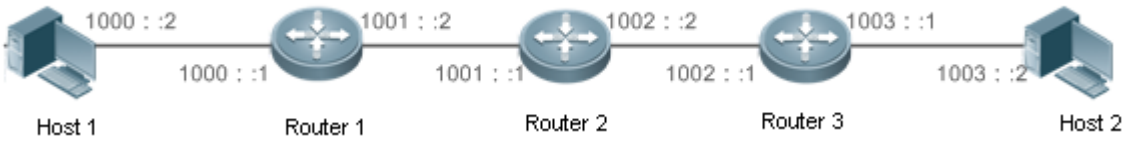
Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. RFC 2460 defines the Type 0 routing header (similar to the loose source routing option of IPv4). The format of the Type 0 routing header is as follows:

Figure 1-14



The following example describes the application of the Type 0 routing header, as shown in Figure 1-15.

Figure 1-15



Host 1 sends Host 2 a packet specifying the intermediate nodes Router 2 and Router 3. The following table lists the changes of fields related to the IPv6 header and routing header during the forwarding process.

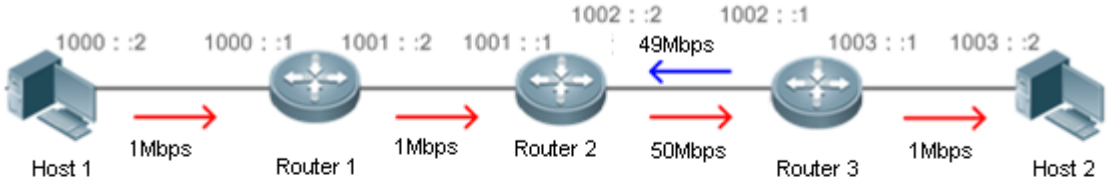
Transmission Node	Fields in the IPv6 Header	Fields Related to the Type 0 Routing Header
Host 1	Source address=1000::2 Destination address=1001::1 (Address of Router 2)	Segments Left=2 Address 1=1002::1 (Address of Router 3) Address 2=1003::2 (Address of Host 2)
Router 1	No change	
Router 2	Source address=1000::2 Destination address=1002::1 (Address of Router 3)	Segments Left=1 Address 1=1001::1 (Address of Router 2) Address 2=1003::2 (Address of Host 2)
Router 3	Source address=1000::2 Destination address=1003::2 (Address of Host 2)	Segments Left=0 Address 1=1001::1 (Address of Router 2) Address 1=1002::2 (Address of Router 3)
Host 2	No change	

The forwarding process is as follows:

1. Host 1 sends a packet in which the destination address is Router 2's address 1001::1, the Type 0 routing header is filled with Router 3's address 1002::1 and Host 2's address 1003::2, and the value of the Segments Left field is 2.
2. Router 1 forwards this packet to Router 2.
3. Router 2 changes the destination address in the IPv6 header to Address 1 in the routing header. That is, the destination address becomes Router 3's address 1002::1, Address 1 in the routing header becomes Router 2's address 1001::1, and the value of the Segments Left field becomes 1. After modification, Router 2 forwards the packet to Router 3.
4. Router 3 changes the destination address in the IPv6 header to Address 2 in the routing header. That is, the destination address becomes Host 2's address 1003::2, Address 2 in the routing header becomes Router 3's address 1002::1, and the value of the Segments Left field becomes 0. After modification, Router 3 forwards the packet to Host 2.

The Type 0 routing header may be used to initiate DoS attacks. As shown in Figure 1-16, Host 1 sends packets to Host 2 at 1 Mbps and forges a routing header to cause multiple round-trips between Router 2 and Router 3 (50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2). At the time, the routing header generates the traffic amplification effect:" 50 Mbps from Router 2 to Router 3 and 49 Mbps from Router 3 to Router 2." Due to this security problem, RFC 5095 abolished the Type 0 routing header.

Figure 1-16



IPv6 Packet
Source Address 1000::2
Destination Address 1001:1

Segments Left in the Type 0 Routing Header: 100
Address 1: 1002::1
Address 2: 1001::1
Address 3: 1002::1
Address 4: 1002::1
...
Address 99: 1002::1
Address 100: 100:3::2

Host 1 sends packets to Host 2, passing through Router 2, Router 3, Router 2, and Router 3, ...
Each packet is sent 50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2.

Related Configuration

Enabling IPv6 Source Routing

- The Type 0 routing header is not supported by default.
- Run the **ipv6 source-route** command in global configuration mode to enable IPv6 source routing.

1.3.7 Restricting the Sending Rate of ICMPv6 Error Messages

Working Principle

The destination node or intermediate router sends ICMPv6 error messages to report the errors incurred during IPv6 data packet forwarding and transmission. There are mainly four types of error messages: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

When receiving an invalid IPv6 packet, a device discards the packet and sends back an ICMPv6 error message to the source IPv6 address. In the case of invalid IPv6 packet attacks, the device may continuously reply to ICMPv6 error messages till device resources are exhausted and thereby fail to properly provide services. To solve this problem, you can restrict the sending rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If the sending rate of ICMPv6 error messages is restricted due to excessive other ICMPv6 error messages, ICMPv6 Packet Too Big messages may be filtered, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages.

Although ICMPv6 Redirect packets are not ICMPv6 error messages, device recommends restricting their rates together with ICMPv6 error messages except Packet Too Big messages.

Related Configuration

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval too-big** command to configure the sending rate of ICMPv6 Packet Too Big messages.

Configuring the Sending Rate of Other ICMPv6 Error Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval** command to configure the sending rate of other ICMPv6 error messages.

1.3.8 IPv6 Hop Limit

Working Principle

An IPv6 data packet passes through routers from the source address and destination address. If a hop limit is configured, it decreases by one every time the packet passes through a router. When the hop limit decreases to 0, the router discards the packet to prevent this useless packet from being unlimitedly transmitted on the network and wasting network bandwidth. The hop limit is similar to the TTL of IPv4.

Related Configuration

Configuring the IPv6 Hop Limit

- The default IPv6 hop limit of a device is 64.
- Run the **ipv6 hop-limit** command to configure the IPv6 hop limit of a device.

1.3.9 Configuring the Device Enabled with IPv6 ND to Allocate Different Prefixes to Different Users

Working Principle

A specific prefix pool can be configured on an interface so that the device assigns different IPv6 prefixes to different users connected to the interface.

Related Configuration

Configuring a Prefix Bound to an Interface

- In global configuration mode, run the **ipv6 local pool** *pool-name ipv6-prefix/prefix-length prefix-length* command to configure the address pool to be assigned.
- In interface configuration mode, run the **ipv6 nd prefix pool** *pool-name* command to configure the name of the prefix pool to which the interface is bound.

1.3.10 Enabling ND Packet Rate Statistics Collection

Working Principle

The device counts the number of ND (RS/RA/NS/NA) messages received or sent by the gateway, and calculates the ND packet rate in a given period of time.

Related Configuration

↘ **Configuring the Interval for ND Packet Rate Statistics Collection**

- In global configuration mode, run the **ipv6 nd rate-statistics interval** *seconds* command.

1.4 Configuration

Configuration	Description and Command	
Configuring an IPv6 Address	⚠ (Mandatory) It is used to configure IPv6 addresses and enable IPv6.	
	ipv6 enable	Enables IPv6 on an interface.
	ipv6 address	Configures the IPv6 unicast address of an interface.
	ipv6 general-prefix	Configures a general IPv6 prefix.
Configuring IPv6 NDP	⚠ (Optional) It is used to set the local address of the link as the source IP address to send neighbor requests.	
	ipv6 ns-linklocal-src	Configures the local address of the link as the source IP address to send neighbor requests.
	⚠ (Optional) It is used to enable IPv6 redirection on an interface.	
	ipv6 redirects	Enables IPv6 redirection on an interface.
	⚠ (Optional) It is used to enable DAD.	
	ipv6 nd dad attempts	Configures the number of consecutive NS packets sent during DAD.
	ipv6 nd dad retry	Configures the interval for address conflict detection.
	⚠ (Optional) It is used to configure ND parameters.	
	ipv6 nd managed-config-flag	Configures the “managed address configuration” flag bit of the RA packet.
	ipv6 nd ns-interval	Configures the interval for the interface to retransmitting NS (Neighbor Solicitation).
	ipv6 nd other-config-flag	Configures “other stateful configuration” flag bit of the RA packet.
	ipv6 nd prefix	Configures the address prefix to be advertised in an RA packet.

Configuration	Description and Command	
	ipv6 nd ra-hoplimit	Configures the hopcount of the RA packet.
	ipv6 nd ra-interval	Configures the interval of sending the RA.
	ipv6 nd ra-lifetime	Configures the device lifetime of the RA sent on the interface.
	ipv6 nd ra-mtu	Configures the MTU of the RA packet.
	ipv6 nd resolve vlan	Configures the device to proactively send NS packets to specific sub-VLANs in the super-VLAN.
	ipv6 nd reachable-time	Configures the reachable time of a neighbor.
	ipv6 nd stale-time	Configures the period for the neighbor to maintain the state.
	ipv6 nd suppress-ra	Enables RA suppression on an interface.
	⚠ (Optional) It is used to configure the maximum number of unresolved ND entries.	
	ipv6 nd unresolved	Configures the maximum number of unresolved ND entries.
	⚠ (Optional) It is used to configure the maximum number of unresolved ND entries.	
	ipv6 nd max-opt	Configures the maximum number of ND options.
	⚠ (Optional) It is used to configure the maximum number of neighbors learned on an interface.	
	ipv6 nd cache interface-limit	Configures the maximum number of neighbors learned on an interface.
Enabling PMTUD	⚠ (Optional) It is used to restrict the MTU of IPv6 packets sent on an interface.	
	ipv6 mtu	Configures the IPv6 MTU.
Enabling IPv6 Source Routing	⚠ (Optional) It is used to enable IPv6 source routing.	
	ipv6 source-route	Configures the device to forward IPv6 packets carrying the routing header.
Configuring the Sending Rate of ICMPv6 Error Messages	⚠ Optional.	
	ipv6 icmp error-interval too-big	Configures the sending rate of ICMPv6 Packet Too Big messages.
	ipv6 icmp error-interval	Configures the sending rates of other ICMPv6 error messages and ICMPv6 Redirect packets.
Configuring the IPv6 Hop Limit	⚠ (Optional) It is used to restrict the hop limit of IPv6 unicast packets sent on an interface.	
	ipv6 hop-limit	Configures the IPv6 hop limit.

1.4.1 Configuring an IPv6 Address

Configuration Effect

Configure the IPv6 address of an interface to implement IPv6 network communication.

Configuration Steps

↘ Enabling IPv6 on an Interface

- (Optional) If you do not want to enable IPv6 by configuring an IPv6 address, run the **ipv6 enable** command.

↘ Configuring the IPv6 Unicast Address of an Interface

- Mandatory.

Verification

Run the **show ipv6 interface** command to check whether the configured address takes effect.

Related Commands

↘ Enabling IPv6 on an Interface

Command	**ipv6 enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IPv6 can be enabled on an interface by two methods: 1) running the **ipv6 enable** command in interface configuration mode; 2) configuring an IPv6 address on the interface. If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

↘ Configuring the IPv6 Unicast Address of an Interface

Command	**ipv6 address** *ipv6-address/prefix-length* **ipv6 address** *ipv6-prefix/prefix-length* **eui-64** **ipv6 address** *prefix-name sub-bits/prefix-length* [**eui-64**]
Parameter Description	*ipv6-address*: indicates the IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits. *ipv6-prefix*: indicates the IPv6 address prefix, which must comply with the address format defined in RFC 4291. *prefix-length*: indicates the length of the IPv6 address prefix, that is, the part representing the network in the IPv6 address. *prefix-name*: indicates the name of the universal prefix. This specified universal prefix is used to create the interface address.

	sub-bits: indicates the subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* parameter. This value is combined with the universal prefix to create the interface address. This value must be in the form documented in RFC 4291. *eui-64*: indicates the created IPv6 address, consisting of the configured address prefix and 64-bit interface ID.
Command Mode	Interface configuration mode
Usage Guide	If an IPv6 interface is created and is Up state, the system automatically generates a link-local address for this interface. The IPv6 address of an interface can also be created by the universal prefix mechanism. That is, IPv6 address = Universal prefix + Sub prefix + Host bits. The universal prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery function of the DHCPv6 client (see the *Configuring DHCPv6*). Sub prefix + Host bits are specified by the *sub-bits* and *prefix-length* parameters in the **ipv6 address** command. If you run the **no ipv6 address** command without specifying an address, all manually configured addresses will be deleted. Run the **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64** command to delete the configured address.

↘ Configuring a General Ipv6 Prefix

Command	**ipv6 general-prefix** *prefix-name ipv6-prefix* | *prefix-length*
Parameter Description	*prefix-name*: specifies the name of a general prefix. *ipv6-prefix*: specifies the network prefix value of a general prefix. This value must be represented in the form of colon hexadecimal notation as documented in RFC 4291. *prefix-length*: specifies the length of a general prefix.
Command Mode	Global configuration mode
Usage Guide	A general prefix can facilitate network numbering. A prefix defined in a general prefix can be referenced by a longer specific prefix. When the general prefix changes, the specific prefixes that reference the general prefix will change accordingly. When a network ID changes, only the general prefix needs to be changed. A general prefix can contain several prefixes. The longer specific prefix is typically used for configuring IPv6 addresses on an interface.

Configuration Example

↘ Configuring an IPv6 Address on an Interface

Configuration Steps	Enable IPv6 on the GigabitEthernet 0/1 interface and add IPv6 address 2000::1 to the interface.
	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ipv6 enable Hostname(config-if-GigabitEthernet 0/1)#ipv6 address 2000::1/64

Verification	Run the **show ipv6 interface** command to verify that an address is successfully added to the GigabitEthernet 0/1 interface.
	Hostname(config-if-GigabitEthernet 0/1)#show ipv6 interface gigabitethernet 0/1 interface GigabitEthernet 0/1 is Down, ifindex: 1 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 INET6: 2000::1 [TENTATIVE], subnet is 2000::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

1.4.2 Configuring IPv6 NDP

Configuration Effect

Configure NDP-related attributes, for example, enable IPv6 redirection and DAD.

Notes

RA suppression is enabled on interfaces by default. To configure a device to send RA packets, run the **no ipv6 nd suppress-ra** command in interface configuration mode.

Configuration Steps

↘ **Enabling IPv6 Redirection on an Interface**

- (Optional) IPv6 redirection is enabled by default.
- To disable IPv6 redirection on an interface, run the **no ipv6 redirects** command.

↘ **Configuring the Number of Consecutive NS Packets Sent During DAD**

- Optional.
- To prevent enabling DAD for IPv6 addresses on an interface or modify the number of consecutive NS packets sent during DAD, run the **ipv6 nd dad attempts** command.

Configuring the Reachable Time of a Neighbor

- Optional.
- To modify the reachable time of a neighbor, run the **ipv6 nd reachable-time** command.

Configuring the Address Prefix to Be Advertised in an RA Packet

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.

Enabling/Disabling RA Suppression on an Interface

- Optional.
- If a device needs to send RA packets, run the **no ipv6 nd suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

- Optional.
- If a large number of unresolved ND entries are generated due to scanning attacks, run the **ipv6 nd unresolved** command to restrict the number of unresolved neighbors.

Configuring the Maximum Number of ND Options

- Optional.
- If a device needs to process more options, run the **ipv6 nd max-opt** command.

Configuring the Maximum Number of ND Entries Learned on an Interface

- Optional.
- If the number of IPv6 hosts is controllable, run the **ipv6 nd cache interface-limit** command to restrict the number of neighbors learned on an interface. This prevents ND learning attacks from occupying the memory space and affecting device performance.

Configuring the Interval of Retransmitting NS Packets on an Interface

- Optional.
- If a large number of IPv6 hosts are deployed on a network, you can configure this function to prolong the interval of transmitting NS packets. When the status of many interfaces change, frequent NS packet handling consumes the memory and affect the device performance, resulting in exceptions. This function addresses this issue.

Verification

Run the following commands to check whether the configuration is correct:

- **show ipv6 interface** *interface-type interface-num*: Check whether the configurations such as the redirection function, reachable time of a neighbor, and NS sending interval take effect.

- **show ipv6 interface** *interface-type interface-num* **ra-inifo**: Check whether the prefix and other information configured for RA packets are correct.
- **show run**

Related Commands

Configuring the Global IP Address as the Source Address or Global IP Address to Send Neighbor Requests

Command	**ipv6 ns-linklocal-src**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Managed Address Configuration Flag Bit of RA Packets

Command	**ipv6 nd managed-config-flag**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	This flag determines whether the host that receives the RA packet obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it is used.

Configuring the Interval for the Interface to Retransmit NS (Neighbor Solicitation)

Command	**ipv6 nd ns-interval** *milliseconds*
Parameter Description	*milliseconds*: indicates the interval for retransmitting NS.
Command Mode	Interface configuration mode or global configuration mode
Usage Guide	The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

Configuring the Other Stateful Configuration Flag Bit of the RA Packet

Command	**ipv6 nd other-config-flag**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	With this flag bit set, the flag bit of the RA packet sent by the device is set. After receiving this flag bit, the host uses the DHCPv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

Configuring the Address Prefix to be Advertised in an RA Packet

Command	**ipv6 nd prefix {***ipv6-prefix/prefix-length* | **default**} [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite**{ **infinite** | *preferred-lifetime* }]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]
Parameter Description	*ipv6-prefix*: indicates the network ID of IPv6, which must comply with the address representation format in RFC 4291. *prefix-length*: indicates the length of the IPv6 address prefix. A slash (/) must be added before the prefix. *valid-lifetime*: indicates the period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 30 days. *preferred-lifetime*: indicates the preferred period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 7 days. **at** *valid-date preferred-date*: indicates the valid date and preferred deadline configured for the RA prefix. It uses the format of *dd+mm+yyyy+hh+mm*. **infinite**: indicates that the prefix is permanently valid. **default**: indicates that the default parameter configuration is used. **no-advertise**: indicates that the prefix is not advertised by a router. **off-link**: if the prefix of the destination address in the IPv6 packet sent by a host matches the configured prefix, the device regards the destination address on the same link and directly reachable. This parameter indicates that this prefix does not require on-link determination. **no-autoconfig**: indicates that the prefix in the RA packet received by a host cannot be used for address auto-configuration.
Command Mode	Interface configuration mode
Usage Guide	This command can be used to configure parameters related to each prefix, including whether to advertise this prefix. By default, an RA packet uses the prefix configured by running the **ipv6 address** command. Run the **ipv6 nd prefix** command to add other prefixes. Run the **ipv6 nd prefix default** command to configure the default parameters for an interface. That is, if no parameter is specified when a prefix is added, use the parameters configured in the **ipv6 nd prefix default** command as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, when you use the **ipv6 nd prefix default** command to modify the default parameter configurations, only the prefix configured for the default parameters changes and configurations of the prefix remain the same. **at** *valid-date preferred-date*: You can specify the valid date of the prefix in two methods: 1) specifying a fixed time for each prefix in an RA packet; 2) specifying the deadline. In the second method, the valid date of the prefix in each RA packet decreases till it becomes 0.

Configuring the Hop-count of the RA Packet

Command	**ipv6 nd ra-hoplimit** *value*
Parameter Description	*value*: specifies the hop count of RA packets. The value ranges from 0 to 255 and the default is 64.
Command Mode	Interface configuration mode

Usage Guide	N/A

Configuring the Interval of Sending the RA

Command	**ipv6 nd ra-interval** { *seconds* | **min-max** *min_value max_value* }
Parameter Description	*seconds*: specifies the interval for sending RA packets, in seconds. The default value is 200s. **min-max**: indicates the maximum and minimum interval sending the RA packet in seconds *min_value*: indicates the minimum interval sending the RA packet in seconds *max_value*: indicates the maximum interval sending the RA packet in seconds.
Command Mode	Interface configuration mode
Usage Guide	If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA packet, the actual interval for sending the RA packet will be fluctuated 20% based on the set value. If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Configuring the Device Lifetime of the RA Sent on the Interface

Command	**ipv6 nd ra-lifetime** *seconds*
Parameter Description	*seconds*: specifies the lifetime of a device used as the default device of an interface, in seconds. The value ranges from 0 to 9,000 and the default is 64.
Command Mode	Interface configuration mode
Usage Guide	The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval).

Configuring the MTU of the RA Packet

Command	**ipv6 nd ra-mtu** *value*
Parameter Description	*value*: indicates the MTU value, in the range from 0 to 4294967295.The default value is the same as the IPv6 MTU.
Command Mode	Interface configuration mode
Usage Guide	If it is specified as 0, the RA will not have the MTU option.

Configuring the Device to Proactively Send NS Packets to Specific Sub-VLANs in the Super-VLAN

Command	**ipv6 nd resolve vlan** { *vlan-list* | **none** }
Parameter Description	*vlan-list*: specifies the list of sub-VLANs where NS packets are broadcast. If this parameter is not specified, the device proactively broadcasts NS packets to sub-VLANs of a super-VLAN in a VLAN list. **none**: indicates that NS packets are not broadcast to any sub-VLAN in a super-VLAN.
Command Mode	Global configuration mode

Usage Guide	In the scenario where a super-VLAN has many sub-VLANs, when the device proactively broadcasts and resolves ND packets, the device will send NS packets to the super-VLAN by default. Due to a large number of sub-VLANs, packets will be replicated in large quantities, which will affect the device performance. Most terminals (such as PCs and servers) request the ND neighbor of the gateway before accessing a network. Therefore, there is no need to proactively broadcast NS packets to the sub-VLANs where the terminals reside. For dumb terminals (that do not proactively send NA packets), the **ipv6 nd resolve vlan** *vlan-list* command can be deployed in the VLANs specified by vlan-list. In this case, the device proactively sends NS packets to these VLANs to generate ND entries. After the **ipv6 ns resolve vlan** *vlan-list* command is run, the device broadcasts NS packets to the sub-VLANs specified in vlan-list in the super-VLAN. In particular, if an authentication-free VLAN is configured and the authentication-free VLAN is not specified by vlan-list, NS packets are not broadcast to the authentication-free VLAN. Supported functions vary depending on the product version.

Configuring the Period for the Neighbor to Maintain the State

Command	**ipv6 nd stale-time** *seconds*
Parameter Description	*seconds*: specifies the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds. The default value is 3,600.
Command Mode	Global configuration mode or interface configuration mode
Usage Guide	This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small. This command can be configured in interface or global configuration mode. The command configured in interface configuration mode is preferred. That is, if the aging time of ND packets is configured on an interface, the value takes effect. Otherwise, the value in global configuration mode is used.

Enabling IPv6 Redirection on an Interface

Command	**ipv6 redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All ICMPv6 error messages are transmitted at a limited transmission rate. By default, a maximum number of 10 ICMPv6 error messages are transmitted per second (10 pps).

Configuring the Number of Consecutive NS Packets Sent During DAD

Command	**ipv6 nd dad attempts** *value*
Parameter	*value*: indicates the number of NS packets.

Description	
Command Mode	Interface configuration mode
Usage Guide	You need to enable DAD before configuring an IPv6 address on an interface. Then the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address uses EUI-64, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface). At the time, you must configure a new address and restart the interface to re-enable DAD. When an interface changes from the down state to the up state, DAD is re-enabled for the addresses on this interface.

Configuring the Interval for Address Conflict Detection

Command	**ipv6 nd dad retry** *value*
Parameter Description	*value*: specifies the interval for address conflict detection. The default is 60 seconds. Setting *value* to 0 indicates that the function is disabled.
Command Mode	Global configuration mode
Usage Guide	Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflicting address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

Configuring the Reachable Time of a Neighbor

Command	**ipv6 nd reachable-time** *milliseconds*
Parameter Description	*milliseconds*: indicates the reachable time of a neighbor, ranging from 0 to 3,600,000. The unit is millisecond. The default value is 30s.
Command Mode	Interface configuration mode
Usage Guide	A device detects unreachable neighbors based on the configured reachable time. The shorter the configured reachable time, the faster the device detects unreachable neighbors but the more it consumes network bandwidth and device resources. Therefore, it is not recommended to set this time too small. The configured value is advertised in an RA packet and is also used on the device. If the value is 0, the reachable time is not specified on the device and it is recommended to use the default value.

Enabling/Disabling RA Suppression on an Interface

Command	**ipv6 nd suppress-ra**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To enable RA suppression on an interface, run the **ipv6 suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

Command	**ipv6 nd unresolved** *number*
Parameter Description	*number*: indicates the maximum number of unresolved ND entries.
Command Mode	Global configuration mode
Usage Guide	To prevent malicious scanning attacks from creating a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

Configuring the Maximum Number of ND Options

Command	**ipv6 nd max-opt** *value*
Parameter Description	*value*: indicates the number of supported ND options.
Command Mode	Global configuration mode
Usage Guide	Configure the maximum number of ND options processed by a device, such as link-layer address option, MTU option, redirection option, and prefix option.

Configuring the Maximum Number of ND Entries Learned on an Interface

Command	**ipv6 nd cache interface-limit** *value*
Parameter Description	*value*: indicates the maximum number of neighbors learned by an interface.
Command Mode	Interface configuration mode
Usage Guide	Restricting the number of ND entries learned on an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of ND entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the ND entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

Configuration Example

Enabling IPv6 Redirection on an Interface

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/1.
	Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ipv6 redirects
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Hostname#show ipv6 interface gigabitEthernet 0/1 interface GigabitEthernet 0/1 is Down, ifindex: 1 address(es):

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/1.
	Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ipv6 redirects
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

Configuring IPv6 DAD

Configuration Steps	Configure the interface to send three consecutive NS packets during DAD.
	Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd dad attempts 3
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Hostname#show ipv6 interface gigabitEthernet 0/1 interface GigabitEthernet 0/1 is Down, ifindex: 1 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled

	ND DAD is enabled, number of DAD attempts: 3 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

Configuring Prefix Information in an RA Packet

Configuration Steps	Add a prefix 1234::/64 to interface GigabitEthernet 0/1.
	Hostname(config-if-GigabitEthernet 0/1)#ipv6 nd prefix 1234::/6
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Hostname#show ipv6 interface gigabitEthernet 0/1 ra-info GigabitEthernet 0/1: DOWN (RA is suppressed) RA timer is stopped waits: 0, initcount: 0 statistics: RA(out/in/inconsistent): 0/1/0, RS(input): 0 Link-layer address: 00:00:00:00:00:00 Physical MTU: 1500 ND router advertisements live for 1800 seconds ND router advertisements are sent every 200 seconds<160--240> Flags: !M!O, Adv MTU: 1500 ND advertised reachable time is 0 milliseconds ND advertised retransmit time is 0 milliseconds ND advertised CurHopLimit is 64 Prefixes: <total: 1> 1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)

Configuring the Maximum Number of Unresolved ND Entries

Configuration Steps	Set the maximum number of unresolved ND entries to 200.
	Hostname(config)# ipv6 nd unresolved 200
Verification	Run the **show run** command to check whether the configuration takes effect.

Configuration Steps	Set the maximum number of unresolved ND entries to 200.
	Hostname(config)# ipv6 nd unresolved 200
Verification	Run the **show run** command to check whether the configuration takes effect.
	Hostname#show run ipv6 nd unresolved 200 !

Configuring the Maximum Number of ND Options

Configuration Steps	Set the maximum number of ND options to 20.
	Hostname(config)# ipv6 nd max-opt 20
Verification	Run the **show run** command to check whether the configuration takes effect.
	Hostname#show run ipv6 nd max-opt 20 !

Configuring the Maximum Number of ND Entries Learned on an Interface

Configuration Steps	Set the maximum number of ND entries learned on an interface to 100.
	Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
Verification	Run the **show run** command to check whether the configuration takes effect.
	Hostname#show run ! interface GigabitEthernet 0/1 ipv6 nd cache interface-limit 100 !

Configuring the Interval of Retransmitting NS Packets on an Interface

Configuration Steps	Configure the interval of retransmitting NS packets on an interface.
	Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ns-interval 2000
Verification	Run the **show running-config** command to display the configuration.

Configuration Steps	Configure the interval of retransmitting NS packets on an interface.
	Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ns-interval 2000
Verification	Run the **show running-config** command to display the configuration.
	Hostname#show running-config ! interface GigabitEthernet 0/1 ipv6 nd ns-interval 2000 !

1.4.3 Enabling PMTUD

Configuration Effect

When sending an IPv6 packet, a host fragments the packet based on the PMTU.

Notes

The IPv6 MTU of an interface must be less than or equal to the interface MTU.

Configuration Steps

↘ **Configuring the IPv6 MTU of an Interface**

- Optional.

↘ **Configuring a Static Path MTU**

- Optional.

↘ **Configuring the Aging Time for a Dynamic Path MTU**

- Optional.

Verification

- Run the **show run** command to check whether the configuration is correct.
- Run the **show ipv6 interface** command to check whether the IPv6 MTU of an interface is correct.
- Capture the locally sent IPv6 packets of which the length exceeds the PMTU. The packet capture result shows that the IPv6 packet is fragmented based on the PMTU.

Related Commands

↘ **Configuring the IPv6 MTU of an Interface**

Command	**ipv6 mtu** *bytes*
Parameter Description	*bytes*: indicates the MTU of an IPv6 packet, ranging from 1280 to 1500. The unit is byte.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the IPv6 MTU of an Interface

Configuration Steps	Change the IPv6 MTU of interface GigabitEthernet 0/1 to 1,300.
	Hostname(config-if-GigabitEthernet 0/1)#ipv6 mtu 1300
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Hostname(config-if-GigabitEthernet 0/1)#show ipv6 interface interface GigabitEthernet 0/ is Down, ifindex: 1 address(es): Mac Address: 00:d0:f8:22:33:47 INET6: FE80::2D0:F8FF:FE22:3347 [TENTATIVE], subnet is FE80::/64 INET6: 1020::1 [TENTATIVE], subnet is 1020::/64 INET6: 1023::1 [TENTATIVE], subnet is 1023::/64 Joined group address(es): MTU is 1300 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

1.4.4 Enabling IPv6 Source Routing

Configuration Effect

RFC 5095 abolished the Type 0 routing header. The device does not support the Type 0 routing header by default. The administrator can run the **ipv6 source-route** command to in global configuration mode to enable IPv6 source routing.

Configuration Steps

Enabling IPv6 Source Routing

- Optional.
- To enable IPv6 source routing, run the **ipv6 source-route** command.

Verification

The device can properly forward packets carrying the Type 0 routing header.

Related Commands

Enabling IPv6 Source Routing

Command	ipv6 source-route
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Since the Type 0 header may cause the device prone to DoS attacks, the device does not forward IPv6 packets carrying the routing header by default, but still processes IPv6 packets with itself being the final destination address and the Type 0 routing header.

Configuration Example

Enabling IPv6 Source Routing

Configuration Steps	Enable IPv6 source routing.
	Hostname(config)#ipv6 source-route
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Hostname#show running-config | include ipv6 source-route ipv6 source-route

1.4.5 Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Effect

Configure the sending rate of ICMPv6 error messages.

Configuration Steps

↘ Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- Optional.
- If a device receives many IPv6 packets with the packet length exceeding the IPv6 MTU of the outbound interface and thereby sends many ICMPv6 Packet Too Big messages to consume much CPU resources, run the **ipv6 icmp error-interval too-big** command to restrict the sending rate of this error message.

↘ Configuring the Sending Rate of Other ICMPv6 Error Messages

- Optional.
- If a device receives many illegal IPv6 packets and thereby generates many ICMPv6 error messages, run the **ipv6 icmp error-interval** command to restrict the sending rate of ICMPv6 error messages. (This command does not affect the sending rate of ICMPv6 Packet Too Big messages.)

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Command	**ipv6 icmp error-interval too-big** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If other ICMPv6 error messages are excessive, ICMPv6 Packet Too Big messages cannot be sent, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of

	a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Command	**ipv6 icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuration Example

Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Steps	Set the sending rate of the ICMPv6 Packet Too Big message to 100 pps and that of other ICMPv6 error messages to 10 pps.
	Hostname(config)#ipv6 icmp error-interval too-big 1000 100 Hostname(config)#ipv6 icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Hostname#show running-config | include ipv6 icmp error-interval ipv6 icmp error-interval 1000 10 ipv6 icmp error-interval too-big 1000 100

1.4.6 Configuring the IPv6 Hop Limit

Configuration Effect

Configure the number of hops of a unicast packet to prevent the packet from being unlimitedly transmitted.

Configuration Steps

↘ **Configuring the IPv6 Hop Limit**

- Optional.
- To modify the number of hops of a unicast packet, run the **ipv6 hop-limit value** command.

Verification

- Run the **show running-config** command to check whether the configuration is correct.
- Capture the IPv6 unicast packets sent by a host. The packet capture result shows that the hop-limit field value in the IPv6 header is the same as the configured hop limit.

Related Commands

↘ **Configuring the IPv6 Hop Limit**

Command	**ipv6 hop-limit value**
Parameter Description	*value*: indicates the number of hops of a unicast packet sent by the device. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ **Configuring the IPv6 Hop Limit**

Configuration Steps	Change the IPv6 hop limit of a device to 250.
	Hostname(config)#ipv6 hop-limit 250
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Hostname#show running-config ipv6 hop-limit 254

1.5 Monitoring

Clearing

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

Description	Command
Clears the dynamically learned neighbors.	**clear ipv6 neighbors** [*interface-id*]

Displaying

Description	Command
Displays the IPv6 addresses.	**show ipv6 address** [*interface-name*]
Displays the information of the general prefix.	**show ipv6 general-prefix**
Displays IPv6 information of an interface.	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
Displays neighbor information.	**show ipv6 neighbors** [**verbose**] [*interface-id*] [*ipv6-address*] [**static**]
Displays statistics on IPv6 neighbor tables.	**show ipv6 neighbors statistics** [**all**]
Displays the number of ND entries corresponding to each MAC address	**show ipv6 neighbor statistics per-mac** [*interface-name*] [*mac-address*]
Displays the statistics of IPv6 packets.	**show ipv6 packet statistics** [**total** | *interface-name*]
Displays all IPv6 raw sockets.	**show ipv6 raw-socket** [*num*]
Displays the neighbor routers and the advertisement.	**show ipv6 routers** [*interface-type interface-number*]
Displays all IPv6 sockets.	**show ipv6 sockets**
Displays all IPv6 UDP sockets.	**show ipv6 udp** [**local-port** *num*] [**peer-port** *num*]
Displays statistics on IPv6 UDP sockets.	**show ipv6 udp statistics**

Debugging

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

Description	Command
Debugs ND entry learning.	**debug ipv6 nd**

1 Configuring DHCPv6

1.1 Overview

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows a DHCP server to transfer configurations (such as IPv6 addresses) to IPv6 nodes.

As compared with other IPv6 address allocation methods, such as manual configuration and stateless automatic address configuration, DHCPv6 provides the address allocation, prefix delegation, and configuration parameter allocation.

- DHCPv6 is a stateful protocol for automatically configuring addresses and flexibly adding and reusing network addresses, which can record allocated addresses and enhance network manageability.
- By using the prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and flexible control of station address space.
- The DHCPv6 configuration parameter allocation solves the problem that parameters cannot be obtained through a stateless automatic address configuration protocol and allocates DNS server addresses and domain names to hosts.
- DHCPv6 is a protocol based on the client/server model. A DHCPv6 client is used to obtain various configurations whereas a DHCPv6 server is used to provide various configurations.

The DHCPv6 client usually discovers the DHCPv6 server by reserving multicast addresses within a link; therefore, the DHCPv6 client and DHCPv6 server must be able to directly communicate with each other, that is, they must be deployed within the same link.

Protocols and Standards

- RFC3315: Dynamic Host Configuration Protocol for IPv6
- RFC3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC3736: Stateless DHCP Service for IPv6
- RFC5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.2 Applications

NA

1.3 Features

Basic Concept

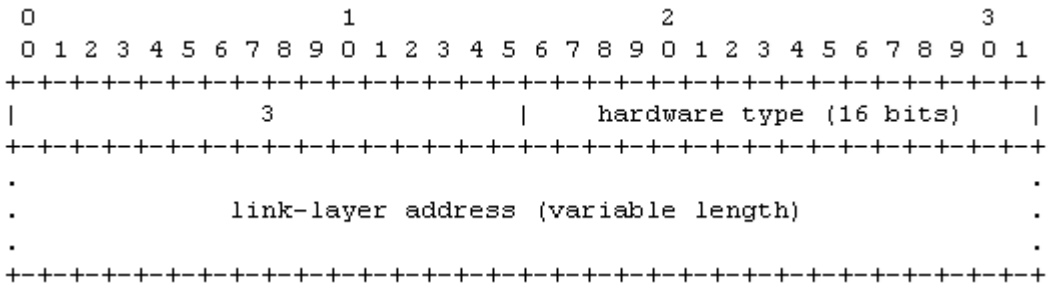
DUID

The DHCP Unique Identifier (DUID) identifies a DHCPv6 device. As defined in RFC3315, each DHCPv6 device (DHCPv6 client, relay or server) must have a DUID, which is used for mutual authentication during DHCPv6 message exchange.

RFC3315 defines three types of DUIDs:

- DUID Based on Link-Layer address plus Time (DUID-LLT).
- DUID Assigned by Vendor Based on Enterprise Number (DUID-EN).
- Link-Layer address (DUID-LL).

DHCPv6 devices use DUID-LLs. The structure of a DUID-LL is as follows:



The values of *DUID-LL*, *Hardware type*, and *Link-layer address* are 0x0003, 0x0001 (indicating the Ethernet), and MAC address of a device respectively.

Identity Association (IA)

A DHCPv6 server allocates IAs to DHCPv6 clients. Each IA is uniquely identified by an identity association identifier (IAID). IAIDs are generated by DHCPv6 clients. A one-to-one mapping is established between IAs and clients. An IA may contain several addresses, which can be allocated by the client to other interfaces. An IA may contain one of the following types of addresses:

- Non-temporary Addresses (NAs), namely, globally unique addresses.
- Temporary Addresses (TAs), which are hardly used.
- Prefix Delegation (PD).

Based on the address type, IAs are classified into IA_NA, IA_TA, and IA_PD (three IA-Types). DHCPv6 servers support only IA_NA and IA_PD.

Binding

A DHCPv6 binding is a manageable address information structure. The address binding data on a DHCPv6 server records the IA and other configurations of every client. A client can request multiple bindings. The address binding data on a server is present in the form of an address binding table with DUID, IA-Type and IAID as the indexes. A binding containing configurations uses DUID as the index.

DHCPv6 Conflict

When an address allocated by a DHCPv6 client is in conflict, the client sends a Decline packet to notify the DHCPv6 server that the address is rebound. Then, the server adds the address to the address conflict queue. The server will not allocate the addresses in the address conflict queue. The server supports viewing and clearing of address information in the address conflict queue.

Packet Type

RFC3315 stipulates that DHCPv6 uses UDP ports 546 and 547 for packet exchange. Specifically, a DHCPv6 client uses port 546 for receiving packets, while a DHCPv6 server and DHCPv6 relay agent use port 547 for receiving packets. RFC3315 defines the following types of packets that can be exchanged among the DHCPv6 server, client, and relay agent:

- Packets that may be sent by a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-request.
- Packets that may be sent by a DHCPv6 server to a DHCPv6 client include Advertise, Reply, and Reconfigure.

DHCPv6 servers do not support the Reconfigure packet.

DHCPv6 clients do not support the Confirm and Reconfigure packets.

Overview

Feature	Description
Requesting\Allocating Addresses	Dynamically obtains/allocates IPv6 addresses in a network in the client/server mode.
Requesting\Allocating Prefixes	Dynamically obtains/allocates IPv6 prefixes in a network in the client/server mode.
Stateless Service	Provides stateless configuration service for hosts in a network.

1.3.1 Requesting\Allocating Addresses

A DHCPv6 client can request IPv6 addresses from a DHCPv6 server.

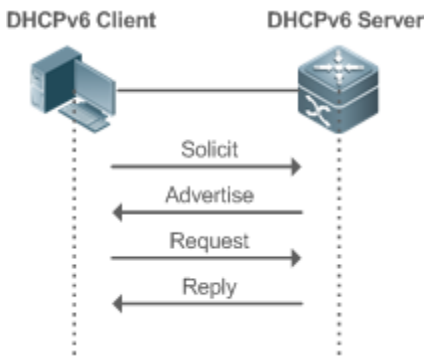
After being configured with available addresses, a DHCPv6 server can provide IPv6 addresses to hosts in the network, record the allocated addresses and improve the network manageability.

Working Principle

Network hosts serve as DHCPv6 clients and DHCPv6 servers to implement address allocation, update, confirmation, release and other operations through message exchange.

Four-Message Exchange

Figure 1-1

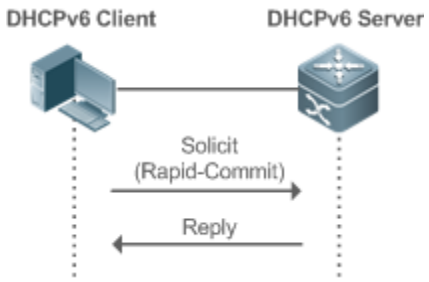


- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix and configuration parameter allocation. All DHCPv6 servers or DHCPv6 relay agents within the link will receive the Solicit message.
- After receiving the Solicit message, a DHCPv6 server will send an Advertise message in the unicast mode if it can provide the information requested in the Solicit message. The Advertise message includes the address, prefix and configuration parameters.
- The DHCPv6 client may receive the Advertise message from multiple DHCPv6 servers. After selecting the most suitable DHCPv6 server, the DHCPv6 client sends a Request message whose destination address is FF02::1:2 and destination port number is 547 to request address, prefix and configuration parameter allocation.
- After receiving the Request message, the DHCPv6 server creates a binding locally and sends a Reply message in the unicast mode. The Reply message includes the address, prefix and configuration parameters that the DHCPv6 server will allocate to the DHCPv6 client. The DHCPv6 client obtains address, prefix or configuration parameters based on the information in the Reply message.

Two-Message Exchange

Two-message exchange can be used to complete address, prefix and parameter configuration for DHCPv6 clients more quickly.

Figure 1-2

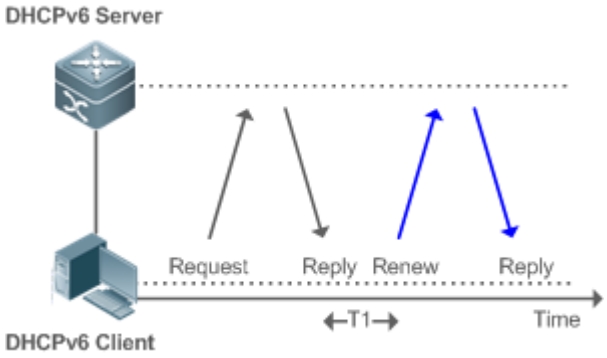


- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix and configuration parameter allocation. The Solicit message contains Rapid Commit.
- If a DHCPv6 server supports the Rapid Commit option, the DHCPv6 server creates a binding locally and sends a Reply message in the unicast mode. The Reply message includes the address, prefix and configuration parameters to be allocated to the DHCPv6 client. The DHCPv6 client completes configuration based on the information in the Reply message.

Update and Rebinding

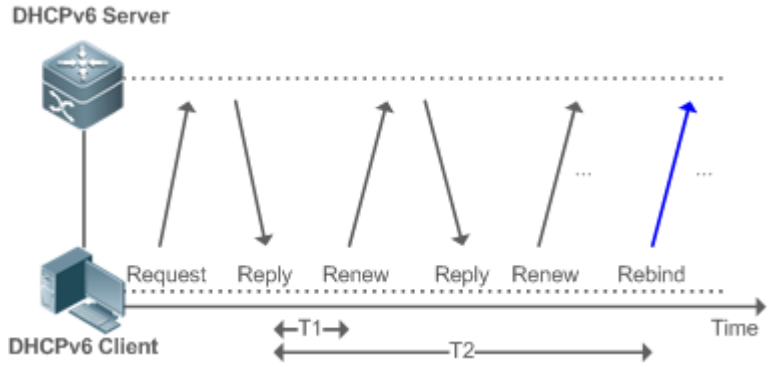
The DHCPv6 server provides the control address and the updated T1 and T2 in the IA of the message sent to the DHCPv6 client.

Figure 1-3



- The DHCPv6 client will send a Renew multicast message to the DHCPv6 server for updating the address and prefix after T1 seconds. The Renew message contains the DUID of the DHCPv6 server and the IA information to be updated.
- After receiving the Renew message, the DHCPv6 server checks whether the DUID value in the Renew message is equal to the DUID value of the local device. If yes, the DHCPv6 server updates the local binding and sends a Reply message in the unicast mode. The Reply message contains the new T1 and other parameter s.

Figure 1-4

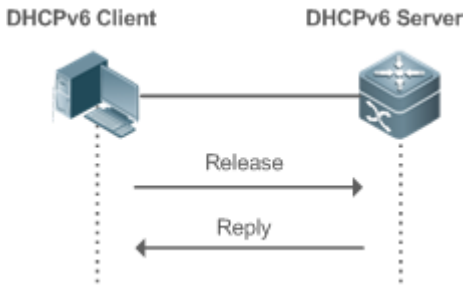


- If no response is received after the DHCPv6 client sends a Renew message to the DHCPv6 server, the DHCPv6 client will send a Rebind multicast message to the DHCPv6 server for rebinding the address and prefix after T2 expires.
- After receiving the Rebind message, the DHCPv6 server (perhaps a new DHCPv6 server) sends a Reply message according to the content of the Rebind message.

Release

If a DHCPv6 client needs to release an address or a prefix, the DHCPv6 client needs to send a Release message to a DHCPv6 server to notify the DHCPv6 server of the released addresses or prefixes. In this way, the DHCPv6 server can allocate these addresses and prefixes to other DHCPv6 clients.

Figure 1-5



- After receiving the Release message, the DHCPv6 server removes the corresponding bindings based on the addresses or prefixes in the Release message, and sends a Reply message carrying the state option to the DHCPv6 client.

Confirmation

After moving to a new link (for example, after restart), a DHCPv6 client will send a Confirm message to the DHCPv6 server on the new link to check whether the original addresses are still available.

Figure 1-6

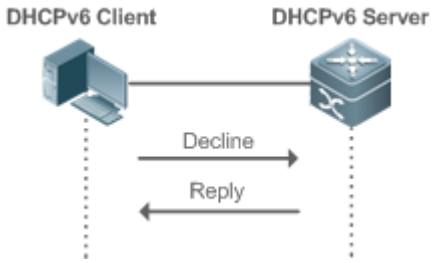


- After receiving the Confirm message, the DHCPv6 server performs confirmation based on the address information in the Confirm message, and sends a Reply message carrying the state option to the DHCPv6 client. If the confirmation fails, the DHCPv6 client may initiate a new address allocation request.

DHCPv6 Conflict

If the DHCPv6 client finds that the allocated addresses have been used on the link after address allocation is completed, the DHCPv6 client sends a Decline message to notify the DHCPv6 server of the address conflict.

Figure 1-7



- The DHCPv6 client includes the IA information of the conflicted addresses in the Decline message.
- After receiving the Decline message, the DHCPv6 server marks the addresses in the Decline message as "declined" and will not allocate these addresses . Then, the DHCPv6 server sends a Reply message carrying the state option to the DHCPv6 client. You can manually clear addresses marked as "declined" to facilitate re-allocation.

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable or disable the DHCPv6 server function for the interface.

The DHCPv6 server function must be enabled on a layer-3 interface.

Allocating Addresses Through the DHCPv6 Server

- You can run the **ipv6 dhcp pool** command to create a configuration pool.
- You can run the **iana-address** command to configure addresses to be allocated and the **preferred lifetime** and **valid lifetime** values.

Clearing Conflicted Addresses Through the DHCPv6 Server

- By default, the DHCPv6 server does not clear conflicted addresses that are detected.
- You can run the **clear ipv6 dhcp conflict** command to clear conflicted addresses so that these addresses can be reused.

Enabling the DHCPv6 Client Address Request Function on an Interface

- By default, an interface is not enabled with the DHCPv6 client address request function.
- You can run the **ipv6 dhcp client ia** command to enable or disable the DHCPv6 client address request function for the interface.

The DHCPv6 client address request function is effective only on a layer-3 interface.

1.3.2 Requesting\Allocating Prefixes

Configure available prefixes on the DHCPv6 server. By using the prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and flexible control of station address space.

Working Principle

Downlink network devices serve as DHCPv6 clients to exchange messages with the DHCPv6 server to implement address allocation, update, release and other operations. Downlink network devices obtain, update, rebind and release prefixes by using the four-/two-message exchange mechanism similar to that for allocating addresses. However, prefix allocation is different from address allocation in the following aspects:

- In message exchange using the prefix delegation, the Confirm and Decline messages are not used.
- If a DHCPv6 client moves to a new link and needs to check whether the prefix information is available, it performs confirmation through Rebind and Reply message exchange.
- The IA type in various messages is IA_PD.

For the message exchange using the prefix delegation, refer to the section "Requesting/Allocating Addresses".

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable or disable the DHCPv6 server function for the interface.

The DHCPv6 server function is effective only on a layer-3 interface.

Prefix Delegation of the DHCPv6 Server

- By default, the DHCPv6 server has no address pool and is not configured with prefixes.
- You can run the **ipv6 dhcp pool** command to create an address pool.
- You can run the **prefix-delegation** command to allocate specified prefixes to a specific DHCPv6 client.
- You can run the **prefix-delegation pool** command to configure a prefix pool so that all prefixes requested by the DHCPv6 client are allocated from this pool.

Enabling the DHCPv6 Client Prefix Request Function on an Interface

By default, an interface is not enabled with the DHCPv6 client prefix request function.

You can run the **ipv6 dhcp client pd** command to enable or disable the DHCPv6 client prefix request function for the interface.

The DHCPv6 client prefix request function is effective only on a layer-3 interface.

1.3.3 Stateless Service

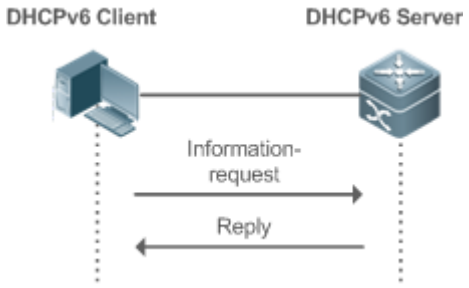
When a DHCPv6 client needs only configuration parameters, the DHCPv6 stateless service can be used to obtain related configuration parameters which cannot be obtained through a stateless automatic address configuration protocol, such as the DNS server address.

Working Principle

Network hosts serve as DHCPv6 clients to exchange messages with the DHCPv6 server to obtain and update configuration parameters.

Message Exchange Using the Stateless Service

Figure 1-8



- A DHCPv6 client sends an Information-request message to a DHCPv6 server to request stateless messages. Usually, this message does not contain the DUID of the specified DHCPv6 server.
- The DHCPv6 server sends a Reply message containing the configuration parameters to the DHCPv6 client.

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable or disable the DHCPv6 server function for the interface.

⚠ The DHCPv6 server function is effective only on a layer-3 interface.

Stateless Service of a DHCPv6 Server

- By default, the DHCPv6 server has no pool and is not configured with configuration parameters.
- You can run the **ipv6 dhcp pool** command to create an address pool.
- You can run the **dns-server** command to add a DNS server.
- You can run the **domain-name** command to add a domain name.
- You can run the **option52** command to add the IPv6 address of the CAPWAP AC.
- You can run the **excluded-address** command to add an excluded address on a DHCPv6 server.

Stateless Service of a DHCPv6 Client

- By default, an interface is not enabled with the stateless service of the DHCPv6 client.
- If a host receives an RA message containing the O flag, it will enable the stateless service.

1.4 Configuration

Configuration	Description and Command	
Configuring the DHCPv6 Server	⚠ (Mandatory) Create a DHCPv6 server configuratio pool.	
	ipv6 dhcp pool	Configures a configuration pool for a DHCPv6 server.
	⚠ (Optional) It is used to allocate prefixes.	
	prefix-delegation	Configures prefixes of statically bound addresses on the DHCPv6 server.
	prefix-delegation pool	Configures the DHCPv6 server to allocate prefixes from a local prefix pool.
	ipv6 local pool	Configures a local IPv6 prefix pool.
	⚠ (Optional) It is used to allocate configuration parameters.	
	dns-server	Configures the DNS server on the DHCPv6 server.

Configuration	Description and Command	
	domain-name	Configures the domain name of the DHCPv6 server.
	option52	Configures the IPv6 address of the CAPWAP AC on the DHCPv6 server.
	excluded-address	Configure excluded addresses on a DHCPv6 server.
	⚠ (Mandatory) It is used to enable the DHCPv6 server service.	
	ipv6 dhcp server	Enables the DHCPv6 server service on an interface.
Configuring the DHCPv6 Client	⚠ (Mandatory) It is used to request addresses or prefixes.	
	ipv6 dhcp client ia	Enables the DHCPv6 client and requests IANA addresses.
	ipv6 dhcp client pd	Enables the DHCPv6 client and requests address prefixes.
	⚠ (Optional) It is used to enable a host that receives an RA message to request stateless service through the DHCPv6 client.	
	ipv6 nd other-config-flag	Sets the O flag in the RA message on the device that sends the RA message so that the host that receives the RA message can request stateless service through the DHCPv6 client.

1.4.1 Configuring the DHCPv6 Server

Configuration Effect

- An uplink device can automatically allocate DHCPv6 addresses, prefixes and configuration parameters to a downlink device.

Notes

- To provide the DHCPv6 server service, you must specify a DHCPv6 server pool.
- The name of the pool cannot be too long.
- When enabling the DHCPv6 server service, you must specify a pool
- Only the Switch Virtual Interface (SVI), routed port and L3 aggregate port (AP) support this configuration.

Configuration Steps

↘ Configuring a DHCPv6 Server pool

- Mandatory.

- Unless otherwise specified, you should configure a pool on all devices that need to provide the DHCPv6 server service.

Configuring the Address Prefixes to Be Allocated on the DHCPv6 Server

- Optional.
- To provide the address allocation service, you should configure address prefixes to be allocated on all devices that need to provide the DHCPv6 server service.

Configuring Prefixes of Static Addresses on the DHCPv6 Server

- Optional.
- To provide the prefix delegation service for statically bound addresses, you should configure prefixes of statically bound addresses on all devices that need to provide the DHCPv6 server service.

Configuring the DHCPv6 Server to Allocate Prefixes from a Local Prefix Pool

- Optional.
- To provide the prefix delegation service, you should specify a local prefix pool on all devices that need to provide the DHCPv6 server service.

Configuring a Local IPv6 Prefix Pool

- Optional.
- To provide the prefix delegation service through a prefix pool, you should specify a local prefix pool on all devices that need to provide the DHCPv6 server service.

Configuring the DNS Server on the DHCPv6 Server

- Optional.
- To allocate DNS servers, you should configure the DNS server on all devices that need to provide the DHCPv6 server service.

Configuring Domain Names on the DHCPv6 Server

- Optional.
- To allocate domain names, you should configure domain names on all devices that need to provide the DHCPv6 server service.

Configuring the IPv6 Address of the CAPWAP AC on the DHCPv6 Server

- Optional.
- To allocate CAPWAP AC information, you should configure the IPv6 address of the CAPWAP AC on all devices that need to provide the DHCPv6 server service.

Enabling the DHCPv6 Server Service

- Mandatory.
- Unless otherwise specified, you should enable the DHCPv6 server service on specific interfaces of all devices that need to provide the DHCPv6 server service.

Verification

The DHCPv6 server allocates addresses, prefixes or configuration parameters for the DHCPv6 client.

- The DHCPv6 client obtains the required information.
- The DHCPv6 server successfully creates a local binding.

Related Commands

Configuring a DHCPv6 Server pool

Command	**ipv6 dhcp pool** *poolname*
Parameter Description	***poolname***: Indicates the name of a user-defined DHCPv6 pool.
Command Mode	Global configuration mode
Usage Guide	Run the **ipv6 dhcp pool** command to create a DHCPv6 server configuratio pool. After configuring this command, you may enter the DHCPv6 pool configuration mode, in which you can configure the pool parameters such as the prefix and DNS server. After creating a DHCPv6 server configuration pool, you can run the **ipv6 dhcp server** command to associate the configuration pool with the DHCPv6 server service on an interface.

Configuring Prefixes of Statically Bound Addresses on the DHCPv6 Server

Command	**prefix-delegation** *ipv6-prefix/prefix-length client-DUID* [*lifetime*]
Parameter Description	*ipv6-prefix/prefix-length*: Indicates an IPv6 address prefix and the prefix length. *client-DUID*: Indicates the DUID of a client. *lifetime*: Sets the time when the client can use this prefix.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **prefix-delegation** command to manually configure a prefix list for an IA_PD of a client and specify the valid time of these prefixes. Use the *client-DUID* parameter to specify the client to which the address prefix is allocated. The address prefix will be allocated to the first IA_PD of the client. After receiving a request for the address prefix from the client, the DHCPv6 server checks whether a static binding is available. If yes, the DHCPv6 server directly returns the static binding. If not, the DHCPv6 server allocates the address prefix from another prefix source.

Configuring the DCHPv6 Server to Allocate Prefixes from a local prefix pool

Command	**prefix-delegation pool** *poolname* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]
Parameter Description	***poolname*:** Indicates the name of a user-defined local prefix pool. **lifetime:** Sets the valid time of the prefix allocated to a client. This keyword must be configured together with *valid-lifetime* and *preferred-lifetime*. *valid-lifetime*: Indicates the valid time of the prefix allocated to the client. *preferred-lifetime*: Indicates the time when a prefix is preferentially allocated to a client.
Command Mode	DHCPv6 pool configuration mode

Usage Guide	Run the **prefix-delegation pool** command to configure a prefix pool for a DHCPv6 server to allocate prefixes to clients. The **ipv6 local pool** command is used to configure a prefix pool. When receiving a prefix request from a client, the DHCPv6 server selects an available prefix from the prefix pool and allocates the prefix to the client. When the client does not use this prefix, the DHCPv6 server retrieves the prefix .

Configuring a Local IPv6 Prefix Pool

Command	**ipv6 local pool** *poolname prefix/prefix-length assigned-length*
Parameter Description	*poolname*: Indicates the name of a local prefix pool. *prefix/prefix-length*: Indicates the prefix and prefix length. *assigned-length*: Indicates the length of the prefix allocated to a user.
Command Mode	Global configuration mode
Usage Guide	Run the **ipv6 local pool** command to create a local prefix pool. If the DHCPv6 server needs prefix delegation, you can run the **prefix-delegation pool** command to specify a local prefix pool. Afterwards, prefixes will be allocated from the specified local prefix pool.

Configuring the DNS Server on the DHCPv6 Server

Command	**dns-server** *ipv6-address*
Parameter Description	*ipv6-address*: Indicates the IPv6 address of the DNS server.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **dns-server** command for multiple times to configure multiple DNS server addresses. A new DNS server address will not overwrite old DNS server addresses.

Configuring Domain Names on the DHCPv6 Server

Command	**domain-name** *domain*
Parameter Description	*domain*: Defines a domain name to be allocated to a user.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **domain-name** command for multiple times to create multiple domain names. A new domain name will not overwrite old domain names.

Configuring the option52 on the DHCPv6 Server

Command	**option52** *ipv6-address*
Parameter Description	*ipv6-address*: Specifies the IPv6 address of the CAPWAP AC.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **option52** command to configure IPv6 addresses for the multiple CAPWAP ACs. A new CAPWAP AC IPv6 address will not overwrite old IPv6 addresses.

Enabling the DHCPv6 Server Service

Command	**ipv6 dhcp server** *poolname* **[rapid-commit] [preference** *value***]**
Parameter Description	*poolname*: Indicates the name of a user-defined DHCPv6 pool. **rapid-commit:** Permits the two-message exchange process. **preference** *value***:** Configures the priority of the advertise message, ranging from 0 to 255. The default value is 0.
Command Mode	Interface configuration mode
Usage Guide	Run the **ipv6 dhcp server** command to enable the DHCPv6 service on an interface. When the **rapid-commit** keyword is configured, the two-message exchange with a client is permitted during allocation of address prefixes and other configurations. After this keyword is configured, if the Solicit message from a client contains the **rapid-commit** option, the DHCPv6 server will send a Reply message directly. If **preference** is set to a non-0 value, the advertise message sent by the DHCPv6 server contains the **preference** option. The **preference** field affects the server selection by a client. If an advertise message does not contain this field, the value of **preference** is considered **0**. If the value of **preference** received by the client is 255, the client sends a request to the server immediately to obtain configurations. The DHCPv6 client, server, and relay functions are mutually exclusive. An interface can be configured with only one function at a time.

Configuration Example

Configuring the DHCPv6 Server

Configuration Steps	● Configure a pool named "pool1". ● Configure prefixes of statically bound addresses on the DHCPv6 server. ● Configure two DNS servers. ● Configure the domain name. ● Enable the DHCPv6 server service on an interface.
	Hostname# configure terminal Hostname(config)# ipv6 dhcp pool pool1 Hostname(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac Hostname(config-dhcp)# dns-server 2008:1::1 Hostname(config-dhcp)# dns-server 2008:1::2 Hostname(config-dhcp)# domain-name example.com Hostname(config-dhcp)#exit Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if)# ipv6 dhcp server pool1
Verification	● Run the **show ipv6 dhcp pool** command to display the created pool.

	Hostname# show ipv6 dhcp pool DHCPv6 pool: pool1 Static bindings: Binding for client 0003000100d0f82233ac IA PD prefix: 2008:2::/64 preferred lifetime 3600, valid lifetime 3600 IANA address range: 2008:50::1/64 -> 2008:50::ffff:ffff:ffff:ffff/64 preferred lifetime 1000, valid lifetime 2000 DNS server: 2008:1::1 DNS server: 2008:1::2 Domain name: example.com

Common Errors

- The specified pool name is too long.
- The number of the pools exceeds the system limit (256).
- The configuration is performed on other interfaces than the Switch Virtual Interface (SVI), routed port and L3 AP port.
- The number of interfaces configured with the DHCPv6 server service exceeds the system limit (256).
- The specified value of **valid lifetime** is smaller than that of **preferred lifetime**.
- An invalid IA_NA address is specified.
- The number of address ranges exceeds the system limit (20).
- When prefixes of statically bound addresses are configured, the specified DUIDs are too long.
- The number of prefixes of statically bound addresses exceeds the system limit (1024).
- When a local prefix pool is configured, the specified value of **valid lifetime** is greater that of **preferred lifetime**.
- The number of DNS servers exceeds the system limit (10).
- The number of domain names exceeds the system limit (10).
- The number of option52 addresses exceeds the system limit (10).

1.4.2 Configuring the DHCPv6 Client

Configuration Effect

- Enable a device to automatically request IPv6 addresses or related parameters from a server.

Notes

- The configuration must be performed on layer-3 interfaces.

Configuration Steps

Enabling the DHCPv6 Client and Requesting IANA Addresses

- Mandatory.
- Unless otherwise specified, you should enable the DHCPv6 client address request function on all devices that need to request addresses.

Enabling the DHCPv6 Client and Requesting Address Prefixes

- Mandatory.
- Unless otherwise required, the DHCPv6 Client Prefix Request feature should be enabled on each device that requires a DHCPv6 request prefix.

Enabling the Stateless Service of the DHCPv6 Client

- It is mandatory if the DHCPv6 client needs to obtain configuration parameters.

Verification

- Check whether the interface is enabled with the DHCPv6 client and check the addresses, prefixes and other configuration obtained on the interface.

Related Commands

Enabling the DHCPv6 Address Request Function

Command	**ipv6 dhcp client ia** [**rapid-commit**]
Parameter Description	**rapid-commit:** Permits the simplified message exchange process.
Command Mode	Interface configuration mode
Usage Guide	If the DHCPv6 client mode is not enabled, this command will enable the DHCPv6 client mode on the interface. After the **ipv6 dhcp client ia** command is configured, an IANA address request will be sent to the DHCPv6 server. The **rapid-commit** keyword permits the two-message exchange process between the client and server. If this keyword is configured, the Solicit message sent by the client contains the **rapid-commit** option.

Enabling the DHCPv6 Client Prefix Request

Command	**ipv6 dhcp client pd** *prefix-name* [**rapid-commit**]
Parameter Description	*prefix-name*: Indicates a IPv6 general prefix. **rapid-commit:** Permits the simplified message exchange process.
Command Mode	Interface configuration mode
Usage Guide	If the DHCPv6 client mode is not enabled, this command will enable the DHCPv6 client mode on the interface.

	After the **ipv6 dhcp client pd** command is configured, a prefix request will be sent to the DHCPv6 server. After receiving the prefix, the client will save the prefix in the IPv6 general prefix pool. Then, other commands and applications can use this prefix. The **rapid-commit** keyword permits the two-message exchange process between the client and server. If this keyword is configured, the Solicit message sent by the client contains the **rapid-commit** option.

Configuring Stateless Service

Command	**ipv6 nd other-config-flag**
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	Configure this command on a host that sends the RA message. Then, the host that receives the RA message obtains stateless configurations through the DHCPv6 client.

Configuration Example

Enabling the DHCPv6 Address Request Function

Configuration Steps	● Configure the DHCPv6 client address request function on an interface.
	Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client ia
Verification	● Run the **show ipv6 dhcp interface** command to display whether the interface is enabled with the DHCPv6 client.
	Hostname#show ipv6 dhcp interface gigabitethernet 0/1 GigabitEthernet 0/1 is in client mode Rapid-Commit: disable

Enabling the DHCPv6 Client Prefix Request

Configuration Steps	● Configure the DHCPv6 client prefix request function on an interface.
	Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client pd pd_name
Verification	● Run the **show ipv6 dhcp interface** command to display whether the interface is enabled with the DHCPv6 client.
	Hostname#show ipv6 dhcp interface gigabitethernet 0/1

	GigabitEthernet 0/1 is in client mode Rapid-Commit: disable

Enabling the DHCPv6 Stateless Service

Configuration Steps	● Configure this command on an interface that sends the RA message.
	Hostname# configure terminal Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd other-config-flag
Verification	● Run the **show ipv6 dhcp interface** command to display whether an interface of the host obtains configuration parameters.
	Hostname#show ipv6 dhcp interface gigabitethernet 0/2 GigabitEthernet 0/2 is in client mode DNS server: 2001::1 Rapid-Commit: disable

Common Errors

- The DHCPv6 client address request is enabled on non-layer-3 interfaces.
- The DHCPv6 address request is enabled on interfaces enabled with the DHCPv6 relay or DHCPV6 server.
- The DHCPv6 client prefix request is enabled on non-layer-3 interfaces.
- The DHCPv6 prefix request is enabled on interfaces enabled with the DHCPv6 relay or DHCPV6 server.

1.5 Monitoring

Clearing

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

Description	Command
Clears DHCPv6 bindings.	**clear ipv6 dhcp binding** [*ipv6-address*]
Clears DHCPv6 server statistics.	**clear ipv6 dhcp server statistics**
Clears conflicted addresses on the DHCPv6 server.	**clear ipv6 dhcp conflict** { *ipv6-address* | * }
Restarts the DHCPv6 client.	**clear ipv6 dhcp client** *interface-type interface-number*

Displaying

Description	Command
Displays the DUID of a device.	**show ipv6 dhcp**

Displays address bindings on the DHCPv6 server.	**show ipv6 dhcp binding** [*ipv6-address*]
Displays DHCPv6 interface.	**show ipv6 dhcp interface** [*interface-name*]
Displays DHCPv6 pool.	**show ipv6 dhcp pool** [*poolname*]
Displays conflicted DHCPv6 addresses.	**show ipv6 dhcp conflict**
Displays the statistics on the DHCPv6 server.	**show ipv6 dhcp server statistics**
Displays the local IPv6 prefix pool.	**show ipv6 local pool** [*poolname*]

Debugging

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

Description	Command
Debugs DHCPv6.	**debug ipv6 dhcp** [**detail**]

1 Configuring ND Proxy

1.1 Overview

ND proxy is a feature of an access controller (AC). It can work as a proxy for a device in the wireless local area network (WLAN) to respond to NS requests of another device. Because CSMA/CA is used for communication in a wireless network, ND proxy can prevent NS broadcast packets in one access point (AP) from being sent to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Protocols and Standards

N/A

1.2 Applications

Application	Description
ND Proxy Service in the WLAN	AC acts as a proxy to respond to NS requests of any device in the WLAN.

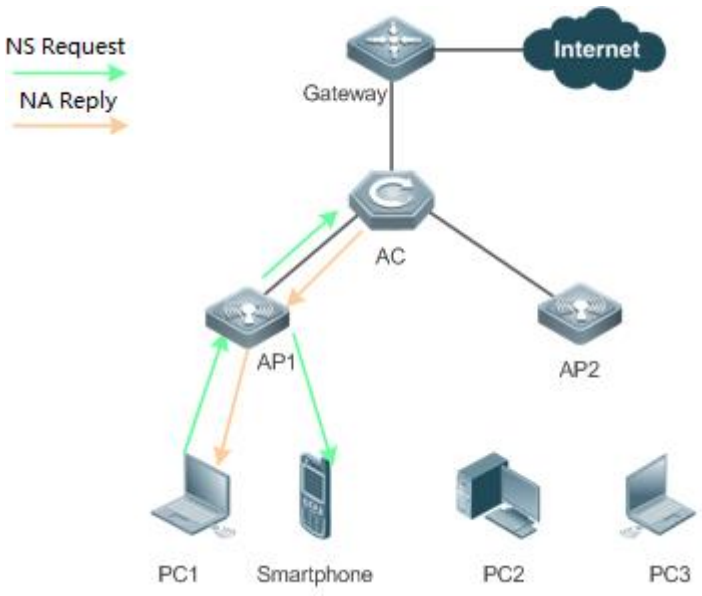
1.2.1 ND Proxy Service in the WLAN

Scenario

In centralized forwarding mode of the fit AP, AC acts a proxy for NS requests of any device in the WLAN.

- The AC needs to learn the MAC address of devices in the WLAN before responding to this device.

Figure 1-1



Remarks	The above figure is the flowchart of the ND request packets that wireless STAs send to the gateway or

	other devices in centralized forwarding mode of the fit AP in the WLAN.

Deployment

- Deploy a network consisting of the gateway, AC, APs, and wireless STAs. Using the ND proxy function (enabled by default), AC works as a proxy to respond to the NS requests of wireless STAs to prevent the NS broadcast requests from being sent to other APs.
- The ND proxy runs on AC and is transparent to users. You can run this function without any other configurations. For details about how to deploy the network environment, refer to the chapter related to wireless networking.

1.3 Features

Basic Concepts

↘ ND Proxy

Layer-2 ND proxy is a feature of AC product. It is also called ND proxy and works as a proxy for a device in the WLAN to respond to the NS requests of another device. Because CSMA/CA is used for communication in a wireless network, ND proxy can prevent NS broadcast packets in one AP from being sent to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Overview

Feature	Description
Layer 2 Wireless ND Proxy	AC works as an ND proxy for wireless STAs to prevent the NS broadcast requests from being sent to other APs.
Static ND Binding	Static ND binding entries are manually configured by administrator. The device will not update the entries and the entries will exist permanently.

1.3.1 Layer 2 Wireless ND Proxy

Working Principle

In typical wireless networking, a wireless STA usually accesses the Internet through an AP and AC. The typical scenario is that, multiple wireless STAs are associated with one AP while multiple APs are associated with one AC. When wireless STAs under one AP connect to those under another AP, or wireless STAs connect to wired STAs, or wired STAs connect to wireless STAs, NS packets must be transmitted through AC, facilitating the implementation of AC's ND proxy function.

The working process of ND proxy is as follows:

1. AC learns the source IP address and source MAC address from the transmitted NS packet to form an ND entry.
2. The AC works as a proxy in the network to respond to NS requests of other users.
3. If the AC does not have the MAC address of the destination host, it multicasts the 802.1Q-compliant NS request.

4. ND replies are forwarded like 802.1Q-compliant Ethernet frames.

As shown in Figure 4-1, PC3 and PC1 obtain the MAC address of the gateway respectively. Assume that this WLAN has one AC, two APs (AP1 and AP2), and four STAs (PC1, PC2, PC3 and smartphone).

1. PC3 initiates an NS request to the IPv6 address of the gateway.
1. AP2 forwards this NS request to PC2 and AC.
2. From this NS request, AC learns the IPv6 and MAC address of PC3 and forwards this NS request to the gateway, AP1, and PC1 and the smartphone under AP1.
3. The gateway sends an NA reply to PC3 through AC. Then AC learns the IPv6 and MAC address of the gateway.
4. PC1 initiates an NS request to the IPv6 address of the gateway.
5. AP1 forwards this NS request to the smartphone and the AC.
6. AC learns the IPv6 and MAC address of PC1 and works as a proxy for the gateway to directly send an NA reply to PC1. (This is because AC has learned the MAC address of the gateway in step 4. Therefore, NS request packets will not be multicast to PC2 and PC3.)

ND Entry Ageout Mechanism

1. When the number of entries is greater than 20000, 10 entries are aged out every one second.
2. When the number of entries is in the range from 10000 to 20000, one entry is aged out every one second,
3. When the number of entries is in the range from 1000 to 10000, one entry is aged out every 10 seconds.
4. When the number of entries is less than 1000, one entry is aged out every 100 seconds.

Related Configuration

↘ Enabling Layer-2 ND Proxy

- By default, Layer-2 ND proxy is enabled.
- Run the **no proxy-nd enable** command to disable Layer-2 ND proxy.

1.3.2 Static ND Binding

Working Principle

The static ND entry is configured by the administrator and will not be updated.

Related Configuration

↘ Configuring Static ND Binding

- No static ND binding are configured.
- Run the **proxy-nd** *ipv6-address vid mac interface-id* command to configure static ND binding.

1.4 Configuration

Configuration	Description and Command	
Enabling Layer 2 ND Proxy	⚠ (Optional) By default, Layer-2 ND proxy is enabled.	
	proxy-nd enable	Enables Layer-2 ND proxy
Configuring Static Layer 2 ND Proxy	⚠ (Optional)	
	proxy-nd *ipv6-address vid mac interface-id*	Configures static ND proxy.

1.4.1 Enabling Layer 2 ND Proxy

Configuration Effect

Enabling Layer 2 ND proxy improves wireless bandwidth efficiency and user experience.

Notes

N/A

Configuration Steps

↘ Enabling Layer 2 ND Proxy

- By default, Layer 2 ND proxy is enabled.
- In a wireless IPv6 scenario, enabling Layer-2 ND proxy on AC to better network bandwidth utilization and user experience.

Verification

Run the **show proxy-nd statistics** command to check whether ND proxy is enabled.

Related Commands

↘ Disabling ND Proxy

Command	**no proxy-nd enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Disabling Layer-2 ND Proxy

Configuration Steps	Disable layer-2 ND proxy.

	Hostname(config)# proxy-nd enable
Verification	Run the show **proxy-nd statistics** command to check if layer-2 ND proxy is enabled.
	Hostname# show proxy-nd statistics Nd Proxy: Enable Total Entry: 100

Common Errors

N/A

1.4.2 Configuring Static Layer 2 ND Proxy

Configuration Effect

Configure static ND proxy to prevent incorrect ND proxy affecting the network.

Notes

N/A

Configuration Steps

Configuring Static ND Proxy

- Optional
- Configure static ND proxy on a device enabled with ND proxy.

Verification

- Run the **show proxy-nd static** or **show running-config** command to check the configuration.

Related Commands

Configuring Static ND Proxy

Command	**proxy-nd** *ipv6-address vid mac interface-id*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Static ND Proxy

Configuratio	Configure static ND proxy.

n Steps	
	Hostname(config)#proxy-nd 2000::1 2 0001.0001.0001 GigabitEthernet 0/1
Verification	Run the **show running-config** command to check static ND proxy configuration.
	Hostname#show running-config ! proxy-nd 2000::1 2 0001.0001.0001 GigabitEthernet 0/1

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the specified ND proxy entry.	**clear proxy-nd** *<ip-address vlan-id>*
Clears all ND proxy entries of the specified VLAN.	**clear proxy-nd**< *interface-id*>
Clears all ND proxy entries	**clear proxy-nd**

Displaying

Description	Command
Displays all ND proxy entries.	**show proxy-nd**
Displays dynamic ND proxy entries.	**show proxy-nd dynamic**
Displays static ND proxy entries.	**show proxy-nd static**
Displays the specified ND proxy entriy.	**show proxy-nd** *<ipv6-address vlan-id>*
Displays the ND proxy statistics.	**show proxy-nd statistics**

Debugging

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

Description	Command
Displays the events of adding, deleting, and updating ND binding entries.	**debug proxy-nd event**
Displays errors in ND packet processing and ND entry binding.	**debug proxy-nd error**

Debugs the preceding command executions.	**debug proxy-nd all**

1 Configuring TCP

1.1 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)

1.2 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 Exceptions	The device checks whether the peer end works normally through TCP.

1.2.1 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 1-1



Deployment

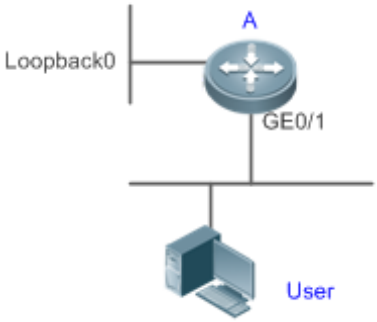
- Enable PMTUD on A and D.

1.2.2 Detecting TCP Connection Exceptions

Scenario

As shown in Figure 1-1, the user logs in to device A through Telnet but is shut down abnormally. If TCP retransmission expires, the user's TCP connection will remain for a long period. In this case, you can use TCP keepalive to rapidly detect TCP connection exceptions.

Figure 1-1



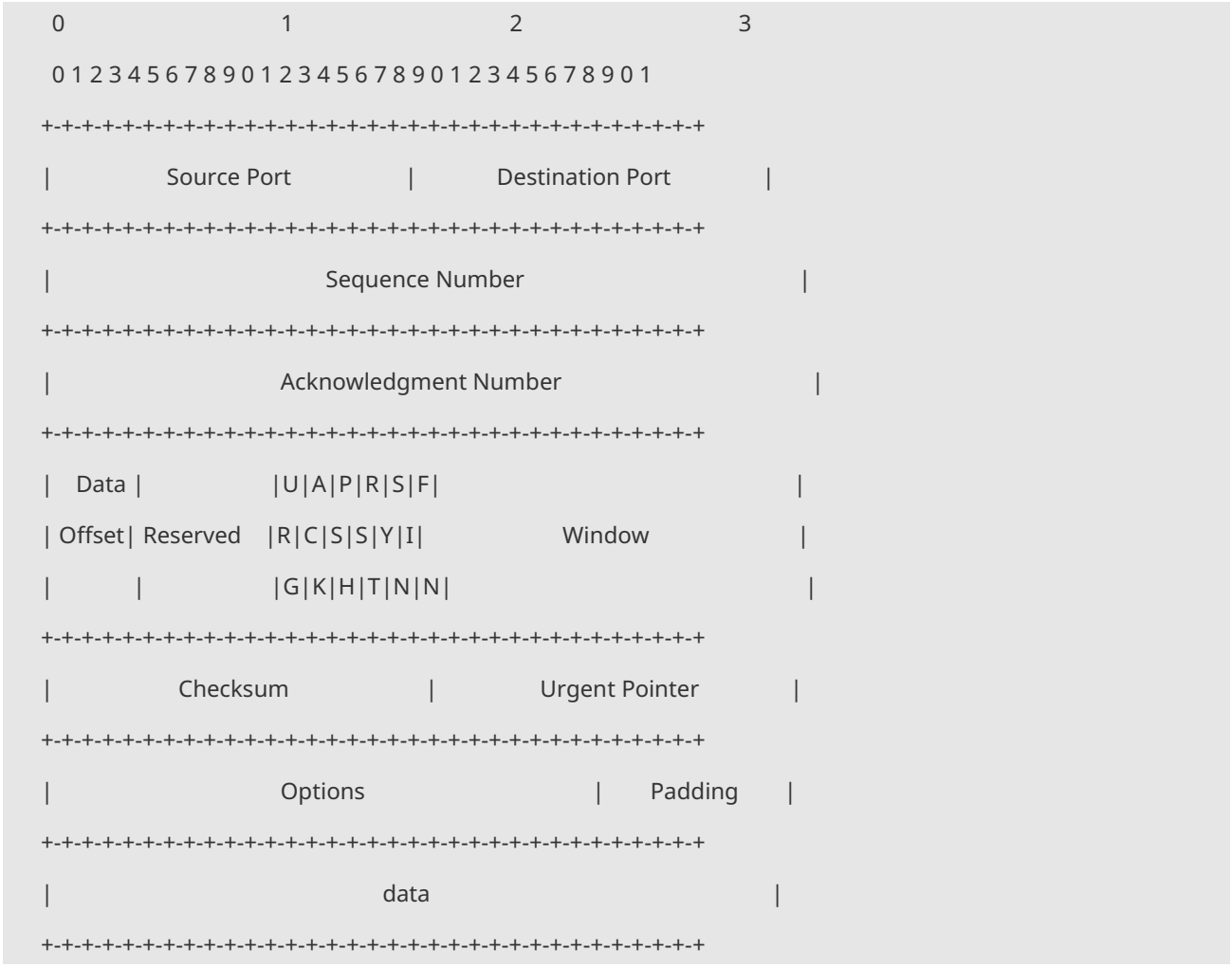
Deployment

- Enable TCP keepalive on device A.

1.3 Features

Basic Concepts

TCP Header Format



- **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.
Configuring MSS Value for SYN Packet	Modify the MSS value in a SYN packet.
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 Function	Check whether the peer works normally.

1.3.1 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.

The **ip tcp syntime-out** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp synwait-time** command.

In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

1.3.2 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.

In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

1.3.3 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.

- The **ip tcp not-send-rst** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **no ip tcp send-reset** command.
- In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

1.3.4 Configuring MSS

Working Principle

The MSS refers to the total amount of data contained in a TCP segment t excluding TCP options.

Three-way handshake is implemented through MSS negotiation. Both parties add the MSS option to SYN packets, indicating the largest amount of data that the local end can handle, namely, the amount of data allowed from the peer. Both parties take the smaller MSS between them as the advertised MSS.

The MSS value is calculated as follows:

- IPv4 TCP: MSS = Outgoing interface MTU –IP header size (20-byte)–TCP header size (20-byte).
- IPv6 TCP: MSS = IPv6 Path MTU –IPv6 header size (40-byte)–TCP header size (20-byte).

- In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.
- The effective MSS is the smaller one between the calculated MSS and the configured MSS.
- If a connection supports certain options, the option length (with **data offset** taken into consideration) should be deducted from an MSS value. For example, 20 bytes for MD5 digest (with **data offset** taken into consideration) should be subtracted from the MSS.

Related Configuration

Configuring MSS

- Run the **ip tcp mss** *max-segment-size* command in global configuration mode to set an MSS. It ranges from 68 to 1000 bytes. By default, the MSS is calculated based on MTU. If an MSS is configured, the effective MSS is the smaller one between the calculated MSS and the configured MSS.
- An excessively small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Choose an MSS value by referring to the interface MTU. If the former is bigger, TCP packets will be fragmented and transmission performance will be reduced.

1.3.5 Configuring MSS Value for SYN Packet

Working Principle

When a client initiates a TCP connection, it negotiates with the server on the total amount of data contained in a TCP segment through the MSS field in TCP SYN packets. The MSS value in the SYN packets indicates the largest amount of data that the server sends in a single and unfragmented piece.

For example, in the following figure, the MSS negotiated between a PC and a HTTP server is 1460, but TCP packets carrying 1460-byte data should be fragmented as they cannot directly pass R1 and R2 connected by a tunnel with an MTU of less than 1500. Modify the MSS value in SYN packets on interfaces (1) and (2) of R2 to enable TCP packets to pass R1 and R2.

Figure 1-2



Related Configuration

Configuring MSS Value for TCPv4 SYN Packets

- By default, the MSS value in TCPv4 SYN packets is not modified.
- Run the **ip tcp adjust-mss** *max-segment-size* command in interface configuration mode to set an MSS, which ranges from 500 to 1460 bytes.
- To avoid packet fragmentation in the case of a small path MTU, you may configure an MSS for TCPv4 SYN packets. The MSS in TCPv4 SYN packets will change to the configured value once the device receives the packets. You may configure an MSS value with reference to the interface MTU.

This configuration applies to a new connection but does not take effect for an existing TCP connection.

Configuring MSS Value for TCPv6 SYN Packets

- By default, the MSS value in TCPv6 SYN packets is not modified.
- Run the **ipv6 tcp adjust-mss** *max-segment-size* command in interface configuration mode to set an MSS for TCPv6 SYN packets, which ranges from 1220 to 1440 bytes.
- To avoid packet fragmentation in the case of a small path MTU, you may configure an MSS for TCPv4 SYN packets. The MSS in TCPv4 SYN packets will change to the configured value once the device receives the packets. You may configure an MSS value with reference to the interface MTU.

This configuration applies to a new TCPv6 connection but does not take effect for an existing TCPv6 connection.

1.3.6 Path MTU Discovery

Working Principle

The Path MTU Discovery f stipulated in RFC1191 is used to discover the smallest MTU in a TCP path to avoid fragmentation, enhancing network bandwidth utilization. The process of TCPv4 Path MTU Discovery is described as follows:

1. The source sends TCP packets with the Don't Fragment (DF) bit set in the outer IP header.
2. If the outgoing interface MTU value of a router in the TCP path is smaller than the IP packet length, the packet will be discarded and an ICMP error packet carrying this MTU will be sent to the source.
3. Through parsing the ICMP error packet, the source knows the smallest MTU in the path (path MTU) is.
4. The size of subsequent data segments sent by the source will not surpass the MSS, which is calculated as follows: TCP MSS = Path MTU – IP header size – TCP header size.

Related Configuration

↘ Enabling Path MTU Discovery

By default, Path MTU Discovery is disabled.

Run the **ip tcp path-mtu-discovery** command to enable PMTUD in global configuration mode.

In version 10.x, the configuration applies to both IPv4 TCP and IPv6 TCP. In version 11.0 or later, it applies to only IPv4 TCP. TCPv6 PMTUD is enabled permanently and cannot be disabled.

1.3.7 TCP Keepalive Function

Working Principle

Enable the TCP keepalive function to check whether the peer works normally. If the remote end of a TCP connection does not send packets to the local end during the idle period, the local end starts sending keepalive packets continuously to the remote end for several times. If no response packet is received, the device considers the remote end as faulty and closes the TCP connection.

Related Configuration

↘ Enabling TCP 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. interval: specifies the keepalive interval. The default value is 75 seconds; times: specifies the maximum number of times for sending keepalive packets. The default value is 6; idle-period: specifies the idle period. The default value is 15 minutes.

In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, the configuration applies to both IPv4 TCP and IPv6 TCP.

1.4 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 keepalive	Configures the TCP keepalive function
	ip tcp adjust-mss	Configures an MSS value for the TCPv4 SYN packets
	ipv6 tcp adjust-mss	Configures an MSS value for TCPv6 SYN packets.
	ip tcp path-mtu-discovery	Enables Path MTU Discovery.
Detecting TCP Connection Exception	(Optional) It is used to detect whether the peer end works normally.	
	ip tcp keepalive	Enables TCP keepalive.

1.4.1 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.

Configuring MSS Value for TCPv4 SYN Packets

- Optional.
- If the MTU between two routers in TCP transmission is small, you may configure an MSS value on the routers.

Configuring MSS Value for TCPv6 SYN Packets

- Optional.
- If the MTU between two routers in TCPv6 transmission is small, you may configure an MSS value on the routers.

Enabling Path MTU Discovery

- Optional.
- Configure this on the both ends of TCP connection.

Verification

N/A

Related Commands

Configuring SYN Timeout

Command	**ip tcp synwait-time** *seconds*
Parameter Description	*seconds*: Indicates SYN packet timeout. It ranges from 5 to 300 seconds. The default is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

Configuring TCP Window Size

Command	**ip tcp window-size** *size*
Parameter Description	*size*: Indicates a TCP window size. It ranges from 128 to (65535 << 14) bytes. The default is 65535 bytes.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

Command	**ip tcp send-reset**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Configuring MSS

Command	ip tcp mss max-segment-size
Parameter Description	*max-segment-size*: Indicates the maximum segment size. It ranges from 68 to 10000 bytes. By default, the MSS is calculated based on MTU.
Command Mode	Global configuration mode
Usage Guide	This command defines the MSS for a TCP communication to be established. The negotiated MSS for a new connection should be smaller than this MSS. If you want to reduce the MSS, run this command. Otherwise, do not perform the configuration.

Configuring the TCP Keepalive Function

Command	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]
Parameter Description	**interval** *num1*: The interval of sending the keepalive packet, in the range from1 to 120 in the unit of seconds, The default is 75. **times** *num2:* Keepalive packet sending times, in the range from 1 to 10. The default is 6. **idle-period** *num3:* Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1800 in the unit of seconds. The default is 900.
Command Mode	Global configuration mode
Usage Guide	The keepalive function enables TCP to detect whether the peer end is operating properly. Suppose the keepalive function is enabled together with default **interval**, **times** and **idle-period** settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.

Configuring MSS Value for TCPv4 SYN Packets

Command	**ip tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size, ranging from 500 to 1460 bytes
Command Mode	Interface configuration mode

Usage Guide	N/A

Configuring MSS Value for TCPv6 SYN Packet

Command	**ipv6 tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: indicates the maximum segment size, ranging from 1220 to 1440 bytes
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Path MTU Discovery

Command	**ip tcp path-mtu-discovery** [**age-timer** *minutes* | **age-timer infinite**]
Parameter Description	**age-timer** *minutes*: Indicates the interval for a new probe after a path MTU is discovered. It ranges from 10 to 30 minutes. The default is 10 minutes. **age-timer infinite**: No probe is implemented after a path MTU is discovered.
Command Mode	Global configuration mode
Usage Guide	The PMTUD is an algorithm documented in RFC1191 aimed to improve bandwidth utilization. When the TCP is applied to bulk data transmission, this function may facilitate transmission performance. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The age timer is a time interval for how often TCP estimates the path MTU with a larger MSS. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You may turn off the timer by setting it to **infinite**.

Configuration Example

Enabling Path MTU Discovery

Configuration Steps	Enable PMTUD for a TCP connection. Adopt the default age timer settings.
	Hostname# configure terminal Hostname(config)# ip tcp path-mtu-discovery Hostname(config)# end
Verification	Run the **show tcp pmtu** command to display the IPv4 TCP PMTU.
	Hostname# show tcp pmtu Number Local Address Foreign Address PMTU 1 192.168.195.212.23 192.168.195.112.13560 1440
	Run the **show ipv6 tcp pmtu** command to display the IPv6 TCP PMTU.

Configuration Steps	Enable PMTUD for a TCP connection. Adopt the default age timer settings.
	Hostname# configure terminal Hostname(config)# ip tcp path-mtu-discovery Hostname(config)# end
Verification	Run the **show tcp pmtu** command to display the IPv4 TCP PMTU.
	Hostname# show ipv6 tcp pmtu Number Local Address Foreign Address PMTU 1 1000::1:23 1000::2.13560 1440

Common Errors

N/A

1.4.2 Detecting TCP Connection Exception

Configuration Effect

- The device checks whether the peer end works normally through TCP.

Notes

N/A

Configuration Steps

Enabling the TCP Keepalive Function

- Optional.

Verification

N/A

Related Commands

Enabling TCP Keepalive

Command	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]
Parameter Description	**interval** *num1*: indicates the interval for sending keepalive packets. The value ranges from 1 to120, in seconds. The default interval is 75 seconds. **times** *num2*: indicates the maximum number of times for sending keepalive packets. The value ranges from 1 to 10. The default value is 6. **idle-period** *num3*: indicates the time when the peer end sends no packets to the local end. The value ranges from 60 to1,800, in seconds. The default value is15 minutes.

Command Mode	Global configuration mode
Usage Guide	You can enable TCP keepalive to check whether the peer works normally. The function is disabled by default. In a scenario where you enable the TCP keepalive function is enabled on a device with the default interval, times and idle period parameter settings, if t he client does not receive any packet from the peer within 15 minutes, the client starts sending keepalive packets to the peer every 75 seconds for 6 ti mes. If the client receives no TCP packets, the TCP connection is considered inactive and then closed.

Configuration Example

↘ Enabling the TCP Keepalive Function

Configuration Steps	Enable TCP keepalive on a device with interval and idle-period set to 3 minutes and 60 seconds respectively. If the user receives no TCP packets from the other end after sending keepalive packets four times, the TCP connection is considered inactive.
	Hostname# configure terminal Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180 Hostname(config)# end
Verification	Log in to a device through telnet, and then shuts down the local device. Run the **show tcp connect** command on the remote device to check the time during which the IPv4 TCP connection is deleted.

↘

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays basic information on IPv4 TCP connection.	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays TCP parameters.	**show tcp parameter**
Displays IPv4 TCP connection statistics.	**show tcp connect statistics**
Displays IPv4 TCP PMTU.	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP port information.	**show tcp port** [*num*]
Displays basic information on IPv6 TCP connection.	**show ipv6 tcp connect** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP connection statistics.	**show ipv6 tcp connect statistics**

Description	Command
Displays IPv6 TCP PMTU.	**show ipv6 tcp pmtu** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP port information.	**show ipv6 tcp port** [*num*]
Displays TCP statistics on received packets, three way handshake and time-wait.	**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.	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv4 TCP connection.	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]
Displays the debugging information on IPv6 TCP packets.	**debug ipv6 tcp packet** [**in** | **out**] [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv6 TCP connection.	**debug ipv6 tcp transactions** [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]

1 Configuring IP REF

1.1 Overview

Ruijie products provide Ruijie Express Forwarding (REF) to achieve software fast forwarding.

REF maintains two tables: forwarding table and adjacency table. The forwarding table is used to store route information. The adjacency table is derived from the ARP table and IPv6 neighbor table, and it contains Layer 2 rewrite (MAC) information for the next hop.

REF is used to actively resolve next hops and implement load balancing.

Protocols and Standards

N/A

1.2 Applications

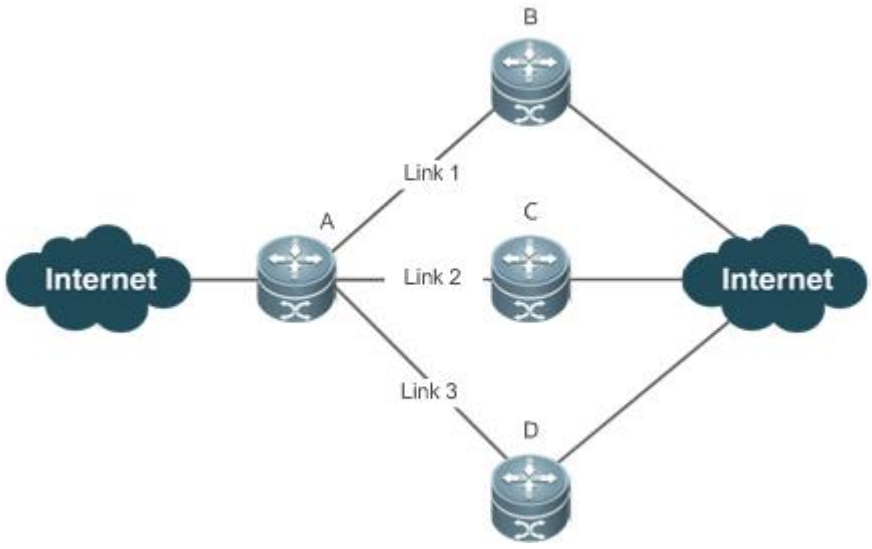
Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among the multiple next hops.

1.2.1 Load Balancing

Scenario

As shown in Figure 1-1, a route prefix is associated with three next hops on device 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 1-1



Remarks	A is a device that runs REF. B, C and D are forwarding devices.

Deployment

- Run REF on device A.

1.3 Features

Basic Concepts

IPv4/IPv6 REF involves the following basic concepts:

Routing table

An IPv4/IPv6 routing table stores routes to the specific destinations and contains the topology information. During packet forwarding, IPv4/IPv6 REF selects packet transmission paths based on the routing table.

Adjacent node

An adjacent node contains output interface information about routed packets, for example, the next hop, the next component to be processed, and the link layer encapsulation. When a packet is matched with an adjacent node, the packet is directly encapsulated and then forwarded. For the sake of query and update, an adjacent node table is often organized into a hash table. To support routing load balancing, the next hop information is organized into a load balance entry. An adjacent node may not contain next hop information. It may contain indexes of next components (such as other line cards and multi-service cards) to be processed.

Active resolution

REF supports next hop resolution. If the MAC address of the next hop is unknown, REF will actively resolve the next hop. IPv4 REF requests the ARP module for next hop resolution while IPv6 REF applies the ND module to resolution.

Packet forwarding path

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined.

Overview

Feature	Description
Load Balancing Policies	Load balancing is configured to distribute traffic load among multiple network links.

1.3.1 Load Balancing Policies

Load balancing is configured to distribute traffic load among multiple network links.

Working Principle

REF supports two load balancing modes. In the REF model, a route prefix is associated with multiple next hops, in other words, it is a multi-path route. The route will be associated with a load balance table and implement weight-based load balancing. When an IPv4/IPv6 packet is matched with a load balance entry based on the longest prefix match, REF performs hash calculation based on the IPv4/IPv6 address of the packet and selects a path to forward the packet.

IPv4/IPv6 REF supports two kinds of load balancing policies: load balancing based on destination IP address, and load balancing based on the source and destination IP addresses.

Related Configuration

↘ Configuring Load Balancing Based on IPv4 Source and Destination Addresses

- By default, load balancing is implemented based on the IPv4 destination addresses.
- Run the **ip ref load-sharing { original | original-only }** command to configure the load balancing.
- After the configuration, load balancing is implemented based on the IPv4 source and destination addresses.

↘ Configuring Load Balancing Based on IPv6 Source and Destination Addresses

- By default, load balancing is implemented based on the IPv6 destination addresses.
- Run the **ipv6 ref load-sharing { original | original-only }** command to configure the load balancing.
- After the configuration, load balancing is implemented based on the IPv6 source and destination addresses.

1.4 Configuration

Configuration	Description and Command	
Configuring Load Balancing Policies	⚠ Optional.	
	ip ref load-sharing { original | original-only }	Enables the load balancing algorithm based on IPv4 source and destination addresses.
	ipv6 ref load-sharing { original | original-only }	Enables the load balancing algorithm based on IPv6 source and destination addresses.

1.4.1 Configuring Load Balancing Policies

Configuration Effect

REF supports the following two kinds of load balancing policies:

- Destination address-based load balancing indicates performing hash calculation based on the destination address of the packet. The path with a greater weight is more likely to be selected. This policy is used by default.
- Implementing load balancing based on the source and destination addresses indicates performing hash calculation based on the source and destination addresses of the packet. The path with a greater weight is more likely to be selected.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration if you want to implement load balancing based on the source and destination IP addresses.
- Perform this configuration on a router that connects multiple links.

Verification

Run the **show ip ref adjacency statistic** command to display the IPv4 load balancing policy.

Run the **show ipv6 ref adjacency statistic** command to display the IPv6 load balancing policy.

Related Commands

Configuring Load Balancing Based on IPv4 Source and Destination Addresses

Command	**ip ref load-sharing { original | original-only }**
Parameter Description	**original**: configures load balancing based on IPv4 source and destination addresses. **original-only**: configures load balancing based on IPv4 source addresses.
Command Mode	Global configuration mode
Usage Guide	N/A

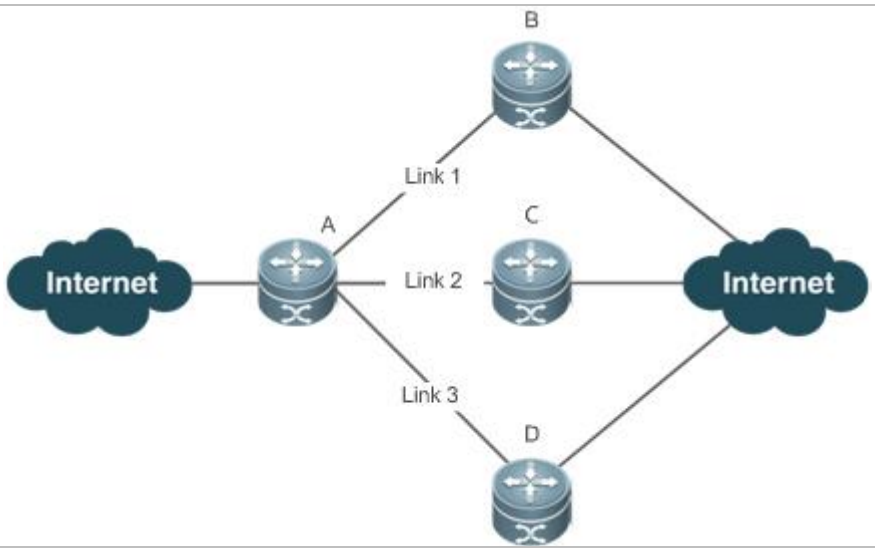
Configuring Load Balancing Based on IPv6 Source and Destination Addresses

Command	**ipv6 ref load-sharing { original | original-only }**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Load Balancing Based on Source and Destination IP Addresses

Scenario **Figure 1-2**	

	
	A route prefix is associated with three next hops on device A, namely, link 1, link 2, and link 3.
Configuration Steps	Configure load balancing based on IPv4 source and destination IP addresses on device A.
A	A# configure terminal A(config)# ip ref load-sharing original
Verification	
	A# show ip ref adjacency statistics adjacency balance table statistic: source-dest-address load-sharing balance: 0 adjacency node table statistic: total : 3 local : 1 glean : 0 forward: 0 discard: 0 mcast : 1 punt : 1 bcast : 0

1.5 Monitoring

Displaying REF Packet Statistics

REF packet statistics includes the number of forwarded packets and the number of packets discarded due to various causes. You can determine whether packets are forwarded as expected by displaying and clearing REF packet statistics.

Description	Command
Displays IPv4 REF packet statistics.	**show ip ref packet statistics**
Clears IPv4 REF packet statistics.	**clear ip ref packet statistics**
Displays IPv6 REF packet statistics.	**show ipv6 ref packet statistics**
Clears IPv6 REF packet statistics.	**clear ipv6 ref packet statistics**

Displaying Adjacency Information

You can run the following commands to display adjacency information:

Description	Command
Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes in IPv4 REF.	**show ip ref adjacency** [**glean** | **local** | *ip-address* | **interface** *interface_type interface_number* **| discard | statistics**]
Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IPv6 address, adjacencies associated with a specified interface, and all adjacent nodes in IPv6 REF.	**show ipv6 ref adjacency** [**glean | local |** *ipv6-address* **| interface** *interface_type interface_number* **| discard | statistics**]

Displaying Active Resolution Information

You can run the following commands to display next hops to be resolved:

Description	Command
Displays the next hop to be resolved .	**show ip ref resolve-list**
Displays the next hop to be resolved.	**show ipv6 ref resolve-list**

Displaying Packet Forwarding Path Information

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined. Run the following commands and specify the IPv4/IPv6 source and destination addresses of a packet. The forwarding path of the packet is displayed, for example, the packet is discarded, submitted to a CPU, or forwarded. Furthermore, the interface that forwards the packet is displayed.

Description	Command
Displays the forwarding path of a packet. oob indicates out-of-band management network.	**show ip ref exact-route** *source-ipaddress dest_ipaddress*
Displays the forwarding path of an IPv6 packet. oob indicates out-of-band, management network.	**show ipv6 ref exact-route** *src-ipv6-address dst-ipv6-address*

Displaying Route Information in an REF Table

Run the following commands to display the route information in an REF table:

Description	Command

Displays route information in the IPv4 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.	**show ip ref route** [**default** | *ip-address mask* | **statistics**]
Displays route information in the IPv6 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.	**show ipv6 ref route** [**default** | **statistics** | *prefix/len*]

1 Configuring FPM

1.1 Overview

The flow platform (FPM) is a platform for the acceleration of packet service processing. Because IP packets have the flow attribute, the FPM provides services with the function to identify the flow attribute of IP packets before service processing, so as to improve service processing efficiency. The FPM is a fundamental platform. It is loaded upon system startup. The configuration commands described in this document are provided to implement FPM configuration and management. In general, the default configuration of the FPM can already meet practical requirements.

The following sections describe the FPM only.

Protocols and Standards

N/A

1.2 Applications

N/A

1.3 Features

Basic Concepts

Flow Entry

A flow entry, as a physical resource for the device to identify and manage all connections of an IP session, records basic information about the current IP session. The corresponding protocols include ICMP, TCP, UDP, and RAWIP.

Overview

Feature	Description
Transparent Transmission of Packets When the Flow Table Is Full	This feature ensures that the existing flows are not interrupted when the flow table is full.
Flow Entry Aging	This feature reclaims invalid flow entries.
Number of Packets Permitted in a Flow	This feature prevents IP packet flooding attacks.
TCP Status Tracing	This feature filters out packets on illegitimate TCP connections.

Packet Threshold for Flows in Various States	This feature performs packet threshold check.
Loose TCP Status Check	This feature allows the establishment of a connection with only ACK packets.

1.3.1 Transparent Transmission of Packets When the Flow Table Is Full

Working Principle

The acceleration of IP service processing relies on a flow table. Flow table resources are configured according to the current product hardware configuration and generally can meet application requirements in an application environment. In some extreme environments, however, flow table resources could be exhausted, causing the failure to establish flows. With this feature, packets are transparently transmitted instead of establishing any flow on wireless products when the flow table is full, and service processing is not accelerated, thereby ensuring that service flows are not interrupted.

1.3.2 Flow Entry Aging

Working Principle

The aging of a flow entry means that the device actively withdraws the flow entry when there is no data exchange in a certain period of time. If a session attack occurs, the flow table will be full, causing the failure to establish sessions. The aging of the flow table is designed to solve this problem. For flow entries of different data types, their aging time shall be set according to actual service requirements. For flows of different service data types, different aging time shall be set according to different states of the flows. For example, the aging time of a TCP flow in SYN status is different from that of a TCP flow in ESTABLISH status. For example again, when a port scanning attack occurs on a network, abundant flow table resources of the system are occupied, and then appropriate aging time can be configured for flows established on these connections according to the states of the flows, so as to effectively reclaim flow entries and avoid flow interruption. Configuring appropriate aging time can help to reduce "useless" flow entries in the flow table while meeting the requirement for exchanging service data flows.

1.3.3 Number of Packets Permitted in a Flow

Working Principle

For each flow in the current status, there is a counter that records the number of packets processed in the flow. An attacker may send a large number of packets of a certain type to wage a traffic attack, in which case other types of packets cannot be processed in time. You can configure the number of packets permitted to pass in a flow in a certain status, so as to solve this problem and meet the requirement for exchanging service data flows.

1.3.4 TCP Status Tracing

Working Principle

A complete handshake process is required for the establishment of a TCP connection; otherwise, the connection is illegitimate or the packets are attack packets. The FPM needs to trace the states of TCP connections, so as to distinguish flows that are established over TCP session connections in various states and determine whether the connections are legitimate. In some special scenarios such as asymmetrical routing, however, the states of TCP connections cannot be traced and then this function should be disabled.

1.3.5 Packet Threshold for Flows in Various States

Working Principle

For a flow in a certain status established over a connection, there is an upper limit on the number of packets permitted on the legitimate connection. If this upper limit is exceeded, a packet flooding attack probably occurs, occupying the forwarding resources of the system. Therefore, you can configure a packet threshold for flows in various states so as to effectively defend against such attacks.

1.3.6 Loose TCP Status Check

Working Principle

A complete handshake process is required for the establishment of a legitimate TCP connection. In some cases such as active/standby switchover, however, probably a handshake process has been performed for the current TCP connection but only no corresponding information exists. In such cases, the system requires only ACK packets. For this purpose, the FPM provides loose TCP status check.

1.4 Configuration

Configuration	Description and Command	
Disabling Transparent Transmission of Packets When the Flow Table Is Full	(Optional) It is used to manage FPM.	
	Ip session direct-trans-disable	Disables the function to transparently transmit packets when the flow table is full.
Configuring the Flow Entry Aging Time	(Optional) It is used to manage FPM.	
	ip session timeout	Configures the flow entry aging time.
Configuring the Number of	(Optional) It is used to manage FPM.	

Packets Permitted in a Flow	**ip session threshold**	Configures the number of packets that can be received for each flow in a certain status.
Enabling the TCP Status Tracing Function	(Optional) It is used to manage FPM.	
	ip session tcp-state-inspection-enable	Enables the TCP status tracing function.
Configuring Packet Threshold Check for Flows in Various States	(Optional) It is used to manage FPM.	
	ip session track-state-strictly	Configures packet threshold for flows in various states.
Configuring Loose TCP Status Check	(Optional) It is used to manage FPM.	
	ip session tcp-loose	Enables the loose TCP status transition check function.

1.4.1 Disabling Transparent Transmission of Packets When the Flow Table Is Full

Networking Requirements

- For some special services such as network address translation (NAT) applied on wireless products, the FPM should not allow the transparent transmission of packets without flow establishment.

Notes

- By default, packets can be transparently transmitted without flow establishment when the flow table is full.

Configuration Steps

- Optional configuration.
- By default, packets can be transparently transmitted without flow establishment when the flow table is full. You can use the **ip session direct-trans-disable** command to disable the function.

Command	**ip session direct-trans-disable**
Parameter Description	N/A
Defaults	Packets can be transparently transmitted without flow establishment when the flow table is full.
Command Mode	Global configuration mode

Usage Guide	Use the **no** form of this command to enable the transparent transmission function.

Verification

- Use the **show run** command to check whether the configuration includes **ip session direct-trans-disable**. If no, the transparent transmission function is enabled.

Configuration Example

Scenario	If the NAT service is required on the current wireless device, you need to disable the transparent transmission function because the NAT service does not allow the transparent transmission of IP packets without flow establishment.
Configuration Steps	Disable transparent transmission of packets without flow establishment when the flow table is full. Hostname# configure terminal Hostname(config)# ip session direct-trans-disable
Verification	Use the **show run** command to verify that the configuration includes **ip session direct-trans-disable**.

Common Errors

N/A

1.4.2 Configuring the Flow Entry Aging Time

Networking Requirements

- Reasonably make use of system flow table resources so as to reduce "useless" flow entries in the flow table and meet the requirement for exchanging service data flows.

Notes

- There is a default aging time upon system initialization, which can meet practical requirements in most scenarios. Therefore, the configuration is optional.
- Because a certain time is required before the system detects the corresponding flow, the actual aging time is slightly later than the configured aging time.

Configuration Steps

↘ Configuring the Aging Time

- Optional configuration.
- By default, a flow entry ages within the default aging time. If the default aging time does not meet the requirement, you can use the **ip session timeout** command to change it. The longer the aging time, the longer the time-to-live (TTL) of the flow entry.

- Perform this configuration on the corresponding forwarding device.

Command	**ip session timeout** {**icmp-closed	icmp-connected	icmp-started	rawip-closed	rawip-connected	rawip-established	rawip-started	tcp-close-wait	tcp-closed	tcp-established	tcp-fin-wait1	tcp-fin-wait2	tcp-syn-receive	tcp-syn-sent	tcp-syn-sent2	tcp-time-wait	udp-closed	udp-started	udp-connected	udp-established**} { *num* }
Parameter Description	**icmp-closed**: Sets the aging time of ICMP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **icmp-connected**: Sets the aging time of ICMP flows in connected status, which is 10 seconds by default and ranges from 5 to 120. **icmp-started**: Sets the aging time of ICMP flows in started status, which is 10 seconds by default and ranges from 5 to 120. **rawip-closed**: Sets the aging time of RAWIP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **rawip-connected**: Sets the aging time of RAWIP flows in connected status, which is 300 seconds by default and ranges from 10 to 300. **rawip-established**: Sets the aging time of RAWIP flows in established status, which is 300 seconds by default and ranges from 10 to 600. **rawip-started**: Sets the aging time of RAWIP flows in started status, which is 300 seconds by default and ranges from 10 to 300. **tcp-close-wait**: Sets the aging time of TCP flows in tcp-close-wait status, which is 60 seconds by default and ranges from 10 to 120. **tcp-closed**: Sets the aging time of TCP flows in tcp-closed status, which is 10 seconds by default and ranges from 5 to 20. **tcp-established**: Sets the aging time of TCP flows in tcp-established status, which is 1,800 seconds by default and ranges from 300 to 604,800. **tcp-fin-wait1**: Sets the aging time of TCP flows in tcp-fin-wait1status, which is 60 seconds by default and ranges from 10 to 120. **tcp-fin-wait2**: Sets the aging time of TCP flows in tcp-fin-wait2status, which is 60 seconds by default and ranges from 10 to 120. **tcp-syn-sent**: Sets the aging time of TCP flows in tcp-syn-sent status, which is 10 seconds by default and ranges from 5 to 30. **tcp-syn_sent2**: Sets the aging time of TCP flows in tcp-syn_sent2 status, which is 10 seconds by default and ranges from 5 to 30. **tcp-syn-receive**: Sets the aging time of TCP flows in tcp-syn-receive status, which is 10 seconds by default and ranges from 5 to 30. **tcp-time-wait**: Sets the aging time of TCP flows in tcp-time-wait status, which is 10 seconds by default and ranges from 5 to 60.

	udp-closed: Sets the aging time of UDP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **udp-connected**: Sets the aging time of UDP flows in connected status, which is 30 seconds by default and ranges from 10 to 300. **udp-established**: Sets the aging time of UDP flows in established status, which is 600 seconds by default and ranges from 120 to 600. **udp-started**: Sets the aging time of UDP flows in started status, which is 10 seconds by default and ranges from 10 to 300. **num**: Sets the aging time
Defaults	Default values apply.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the commands to restore the default aging time.

Verification

- Use the **show run** command to check whether the configuration includes **ip session timeout**. If no, the default aging time applies.

Configuration Example

Scenario	If there are a large number of UDP-established flows which occupy a great space of the flow table on the current forwarding device, you can shorten the aging time of the UDP-established flows to improve aging efficiency.
Configuration Steps	Set the aging time of flows in udp-established status to 120 seconds. Hostname# configure terminal Hostname(config)# ip session 1 2 timeout udp-established 120
Verification	The aging time should be 120 seconds. Use the **show run** command to verify that the configuration contains the following item: ip session 1 2 timeout udp-established 120 This indicates that the aging time is 120 seconds.

Common Errors

N/A

1.4.3 Configuring the Number of Packets Permitted in a Flow

Networking Requirements

- An attacker may send a large number of packets of a certain type to wage a traffic attack, in which case other types of packets cannot be processed in time. You can configure the number of packets permitted in a flow in a certain status, so as to solve this problem and meet the requirement for exchanging service data flows.

Notes

- There is a default packet count upon system initialization, which can meet practical requirements in most scenarios. Therefore, the configuration is optional.
- The check function here is disabled by default. To enable the check function, you need to configure packet threshold check for flows in various states first.

Configuration Steps

- Optional configuration.
- By default, a flow is judged according to the default number of packets permitted to pass in the flow. If the default number of packets permitted to pass does not meet the requirement, you can use the **ip session threshold** command to change the number of packets allowed to pass in the corresponding flow. The greater the value, the more packets permitted to pass in the flow.
- Perform this configuration on each forwarding device as necessary.

Command	**ip session threshold** { icmp-closed | **icmp-started** | rawip-closed | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed** } { *num* }
Parameter Description	**icmp-closed**: Sets the number of packets permitted to pass in each ICMP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. **icmp-started**: Sets the number of packets permitted to pass in each ICMP flow in started status, which is 300 by default and ranges from 5 to 2,000,000,000. **rawip-closed**: Sets the number of packets permitted to pass in each RAWIP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. **tcp-syn-sent**: Sets the number of packets permitted to pass in each TCP flow in syn-send status, which is 10 by default and ranges from 10 to 2,000,000,000. **tcp-syn-receive**: Sets the number of packets permitted to pass in each TCP flow in syn-receive status, which is 20 by default and ranges from 5 to 2,000,000,000. **tcp-closed**: Sets the number of packets permitted to pass in each TCP flow in closed status, which is 20 by default and ranges from 5 to 2,000,000,000. **udp-closed**: Sets the number of packets permitted to pass in each UDP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. *num*: Sets the number of packets permitted to pass

Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the command to restore the default number of packets permitted to pass.

Verification

- Use the **show run** command to check whether the configuration includes **ip session threshold**. If no, the default values about the number of packets permitted to pass apply.

Configuration Example

Scenario	When a large number of ping packets exist on a network, a flooding attack probably occurs. You can configure the number of packets permitted to pass in each ICMP flow in icmp-started status, so as to deny such ping packets.
Configuration Steps	Set the number of packets permitted to pass in each ICMP flow in icmp-started status to 10. Hostname# configure terminal Hostname(config)# ip session 1 2 threshold icmp-started 10
Verification	The number should be 10. Use the **show run** command to verify that the configuration contains the following item: ip session 1 2 threshold icmp-started 10 This indicates that the number of packets permitted to pass in each ICMP flow in icmp-started status is 10.

Common Errors

N/A

1.4.4 Enabling the TCP Status Tracing Function

Networking Requirements

- Perform this configuration to enable the TCP status tracing function.

Notes

- The TCP status tracing function is disabled by default.

Configuration Steps

- Optional configuration.
- The TCP status tracing function is disabled by default. You can use the **ip session** [*dev*] [*slot*] **tcp-state-inspection-enable** command to enable the TCP status tracing function.

Command	**ip session tcp-state-inspection-enable**
Parameter Description	N/A
Defaults	The TCP status tracing function is disabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the TCP status tracing function to default.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-state-inspection-disable**. If no, the TCP status tracing function is enabled.

Configuration Example

Scenario	The current forwarding device is a FW card located in slot 2 of device 1. If the FW card is located on an asymmetrical routing path in the current forwarding environment, you need to disable the TCP status tracing function.
Configuration Steps	Disable the TCP status tracing function on the forwarding device in slot 2 of device 1. Hostname# configure terminal Hostname(config)# ip session 1 2 tcp-state-inspection-disable
Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-state-inspection-disable**.

Common Errors

N/A

1.4.5 Configuring Packet Threshold Check for Flows in Various States

Networking Requirements

- Perform this configuration to enable the packet threshold check function and disable the current flow when packets are unreachable.

Notes

-

Configuration Steps

- Optional configuration.

- You can use the **ip session track-state-strictly** command to enable the strict packet status tracing function.
- The packet threshold check function needs to be enabled in a scenario such as the scenario where attacks are waged using a certain type of packet.

Command	**ip session track-state-strictly**
Parameter Description	N/A
Defaults	The strict packet status tracing function is disabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the default configuration.

Verification

- Use the **show run** command to check whether the configuration includes **ip session track-state-strictly**. If no, the strict packet status tracing function is disabled.

Configuration Example

Scenario	If ICMP flooding attacks occur in the current network environment, packet threshold check is needed. In this case, perform this configuration to enable the packet threshold check function.
Configuration Steps	Enable the strict packet status tracing function on the forwarding device. Hostname# configure terminal Hostname(config)# ip session 1 2 track-state-strictly
Verification	Use the **show run** command to verify that the configuration includes **ip session track-state-strictly**.

Common Errors

N/A

1.4.6 Configuring Loose TCP Status Check

Networking Requirements

- A flow can be directly established with only ACK packets.

Notes

- By default, the establishment of a flow with an ACK packet is allowed on FW products.
- This configuration is optional.

Configuration Steps

- Optional configuration.
- By default, the loose TCP status check function is disabled on FW products. You can use the **ip session tcp-loose** command to enable the loose TCP status check function. By default, the loose TCP status check function is enabled on all wireless and EG products.
- The loose TCP status check function is required on the standby device in a scenario such as active/standby switchover.

Command	**ip session tcp-loose**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the default configuration.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-loose**. If no, the loose TCP status check function is disabled.

Configuration Example

Scenario	Active/standby switchover is required in the current environment. Perform this configuration on the backup device.
Configuration Steps	Enable the loose TCP status check function. Hostname# configure terminal Hostname(config)# ip session 1 2 tcp-loose
Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-loose**.

Common Errors

N/A

1.5 Monitoring

Clearing

If you run the **clear** command while the device is operating, services may be interrupted arising from the loss of important information.

Function	Command
Clears counters about the IPv4 packets.	**clear ip fpm counters**
Clears counters about the IPv6 packets.	**clear ip v6fpm counters**

Displaying

Function	Command
Displays the counters about the IPv4 packets	**show ip fpm counters**
Displays the counters about the IPv6 packets	**show ip v6fpm counters**
Displays IPv4 packet flow information	**show ip fpm flows**
Displays IPv4 packet flow information except specific IPv4 packet flows	**show ip fpm flows filter**
Displays IPv6 packet flow information	**show ip v6fpm flows**
Displays IPv6 packet flow information except specific IPv6 packet flows	**show ip v6fpm flows filter**
Displays IPv4 flow statistics	**show ip fpm statistics**
Displays IPv6 flow statistics	**show ip v6fpm statistics**

Configuring IP Routing

1. Configuring IP Routing Basic

1 Configuring IP Routing Basic

1.1 Overview

The network service module (NSM) manages the routing table, consolidates routes sent by various routing protocols, and selects and sends preferred routes to the routing table. Routes discovered by various routing protocols are stored in the routing table. These routes are generally classified by source into three types:

- Direct route: It is the route discovered by a link-layer protocol and is also called interface route.
- Static route: It is manually configured by the network administrator. A static route is easy to configure and less demanding on the system, and therefore applicable to a small-sized network that is stable and has a simple topology. However, when the network topology changes, the static route must be manually reconfigured and cannot automatically adapt to the topological changes.

1.2 Applications

N/A

1.3 Features

Feature	Description
Route Computation	Generate a valid route on a device.
Optimal Route Selection	Select an optimal route to forward packets.
Default Route	Forward all packets and help reduce the size of a routing table.

1.3.1 Route Computation

Routing Function

Routing functions are classified into IPv4 and IPv6 routing functions. If the routing functions are disabled, a device is equivalent to a host and cannot forward routes.

Dynamic Route

A dynamic routing protocol learns remote routes and dynamically updates routes by exchanging routes with neighbors. If a neighbor is the next hop of a route and this neighbor fails, the route fails as well.

Static Route

On a network with a simple topology, you can configure only static routes to implement network interworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

Whether a static route is active is computed based on the status of the local interface. When the exit interface of a static route is located at layer 3 (L3) and is in Up status (the link status is Up and the IP address is configured), this route is active and can be used for packet forwarding.

1.3.2 Optimal Route Selection

Administrative Distance

When multiple routing protocols generate routes to the same destination, the priorities of these routes can be determined based on the administrative distance. A smaller administrative distance indicates a higher priority.

1.3.3 Default Route

In the forwarding routing table, the route with the destination network segment 0.0.0.0 and the subnet mask 0.0.0.0 is the default route. Packets that cannot be forwarded by other routes will be forwarded by the default route. The default route can be statically configured or generated by a dynamic routing protocol.

Static Default Route

On a L3 device, a static route with the network segment 0.0.0.0 and the subnet mask 0.0.0.0 is configured to generate the default route.

1.4 Configuration

Configuration Item	Description and Command	
Configuring a Static Route	⚠ (Mandatory) It is used to configure a static route entry.	
	ip route	Configures an IPv4 static route.
	ipv6 route	Configures an IPv6 static route.
Configuring a Default Route	⚠ (Optional) It is used to configure the default gateway.	
	ip route 0.0.0.0 0.0.0.0 *gateway*	Configures an IPv4 default gateway on a L3 device.
	ipv6 route ::/0 *ipv6-gateway*	Configures an IPv6 default gateway on a L3 device.
Configuring Route Limitations	⚠ (Optional) It is used to limit the number of equal-cost routes and number of static routes, or disable routing.	
	maximum-paths	Configures the maximum number of equal-cost routes.
	ip static route-limit	Configures the maximum number of IPv4 static routes.
	ipv6 static route-limit	Configures the maximum number of IPv6 static routes.

Configuration Item	Description and Command	
	no ip routing	Disables IPv4 routing.
	no ipv6 unicast-routing	Disables IPv6 routing.

1.4.1 Configuring a Static Route

Configuration Effect

- Generate a static route in the routing table. Use the static route to forward packets to a remote network.

Notes

- If the **no ip routing** command is configured on a L3 switch, you cannot configure IPv4 static routes on this switch, and existing IPv4 static routes will also be deleted. Before the device is restarted, reconfiguring the **ip routing** command can recover the deleted IPv4 static routes. After the device is restarted, deleted IPv4 static routes cannot be recovered.
- If the **no ipv6 unicast- routing** command is configured on a L3 switch, you cannot configure IPv6 static routes on this switch, and existing IPv6 static routes will also be deleted. Before the device is restarted, reconfiguring the **ipv6 unicast- routing** command can recover the deleted IPv6 static routes. After the device is restarted, deleted IPv6 static routes cannot be recovered.

Configuration Steps

↘ Configuring a Static IPv4 Route

Configure the following command on an IPv4-enabled router.

Command	**ip route** *network net-mask* { *ipv4-address* [**global**] | *interface* [*ipv4-address* [**global**]] } [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**]	
Parameter Description	*network*	Indicates the address of the destination network.
	net-mask	Indicates the mask of the destination network.
	ipv4-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv4-address* and *interface,* or both of them. If *ipv4-address* is not specified, a static direct route is configured.
	global	(Optional) Indicates that the next hop address is global.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv4-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag *tag*	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description	(Optional) Indicates the description of the static route. By default, no description

	description-text	is configured. *description-text* is a string of one to 60 characters.
	disabled | **enabled**	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route** *networknet-mask ip-address.*	

↘ Configuring an IPv6 Static Route

Configure the following command on an IPv6-enabled router.

Command	**ipv6 route** *ipv6-prefix/prefix-length* { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*] [**weight** *number*] [**description** *description-text*]	
Parameter Description	*ipv6-prefix*	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	prefix-length	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	Description *description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route** *ipv6-prefix/prefix-length ipv6-address.*	

Verification

- Run the **show ip route** command to display the IPv4 routing table and check whether the configured IPv4 static route takes effect.

- Run the **show ipv6 route** command to display the IPv6 routing table and check whether the configured IPv6 static route takes effect.

1.4.2 Configuring a Default Route

Configuration Effect

- Generate a default route in the routing table. The default route is used to forward packets that cannot be forwarded by other routes.

Notes

- On a L3 switch, run the **ip route 0.0.0.0 0.0.0.0** *gateway* or **ipv6 route ::/0** *ipv6-gateway* command to configure the default gateway.

Configuration Steps

↘ **Configuring the IPv4 Default Gateway on a L3 Switch**

Command	**ip route** 0.0.0.0 0.0.0.0 { *ip-address* [**global**] | *interface* [*ipaddress*] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | [**permanent**] | **tag** *tag* | **weight** *number*]	
Parameter Description	0.0.0.0	Indicates the address of the destination network.
	0.0.0.0	Indicates the mask of the destination network.
	global	(Optional) Indicates that the next hop address is global.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	description *description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	disabled | enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default umber of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	tag *tag*	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
Defaults	By default, no static default route is configured.	
Command	Global configuration mode	

Mode	
Usage Guide	The simplest configuration of this command is **ip route 0.0.0.0 0.0.0.0** *ip-address.*

Configuring the IPv6 Default Gateway

Command	**ipv6 route ::/0** { *ipv6-address* | *interface* [*ipv6-address*] } [*distance* | **description** *description-text* | **tag** *tag* | **weight** *number*] *	
Parameter Description	**::**	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	0	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	Ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	tag *tag*	Specifies the tag value of the static route. The value range is from 1 to 4294967295, and the default value is **0**.
	weight *number*	Specifies the weight of the static route, which must be specified when you configure equal-cost routes. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The value range is from 1 to 8, and the default value is **1**.
Defaults	By default, no static default route is configured.	
Command	Global configuration mode	

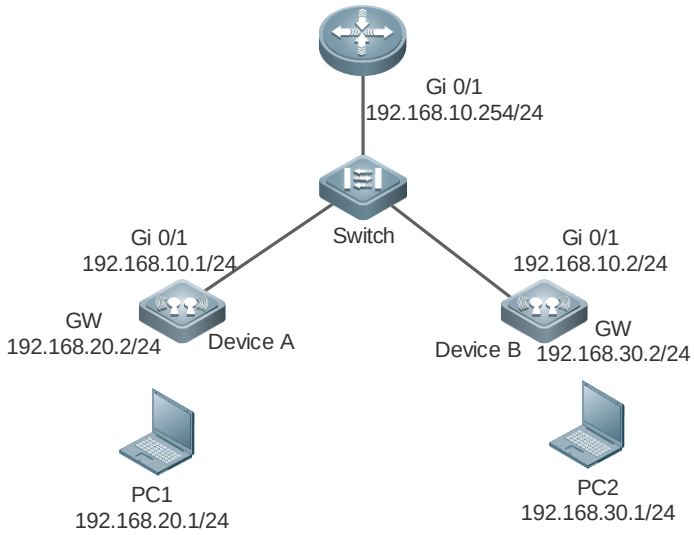
Mode	
Usage Guide	The simplest configuration of this command is **ipv6 route** ::/0 *ipv6-gateway.*

Verification

- Run the **show ip route** or **show ipv6 route** command to display the default route.

Configuration Example

Configuring IPv4 Default Routes on L3 Devices to Implement Network Interworking

Scenario Figure 1-1	
Configuration Steps	• Configure IP addresses on L3 devices.
Device A	DeviceA#configure terminal DeviceA(config)#interface gigabitEthernet 0/1 DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.10.1 255.255.255.0 DeviceA(config-if-GigabitEthernet 0/1)# exit • Configure an IPv4 default gateway. DeviceA(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.254
Device B	DeviceB#configure terminal DeviceB(config)#interface gigabitEthernet 0/1 DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.10.2 255.255.255.0 DeviceB(config-if-GigabitEthernet 0/1)# exit DeviceB(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.254
	DeviceC#configure terminal

Device C	DeviceC(config)#interface gigabitEthernet 0/1 DeviceC(config-if-GigabitEthernet 0/1)# ip address 192.168.10.254 255.255.255.0 DeviceC(config-if-GigabitEthernet 0/1)# exit DeviceC(config)# ip route 192.168.20.0 255.255.255.0 192.168.10.1 DeviceC(config)# ip route 192.168.30.0 255.255.255.0 192.168.10.2
Verification	● Display the routing table.
Device A	Device A# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, EV - BGP EVPN, * - candidate default Gateway of last resort is 192.168.10.254 to network 0.0.0.0 S* 0.0.0.0/0 [1/0] via 192.168.10.254 C 192.168.10.0/24 is directly connected, GigabitEthernet 0/1 C 192.168.10.1/32 is local host. Device A#

1.4.3 Configuring Route Limitations

Configuration Effect

- Limit the number of equal-cost routes and number of static routes, or disable routing.

Notes

N/A

Configuration Steps

↘ **Configuring the Maximum Number of IPv4 Static Routes**

Command	**ip static route-limit** *number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1,024 IP static routes can be configured.	
Command Mode	Global configuration mode	

Usage Guide	Run this command to configure the maximum number of IPv4 static routes. If the maximum number of IPv4 static routes is reached, no more IPv4 static route can be configured.

↘ Configuring the Maximum Number of IPv6 Static Routes

Command	**ipv6 static route-limit** *number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1,000 IPv6 static routes can be configured.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of IPv6 static routes. If the maximum number of IPv6 static routes is reached, no more IPv6 static route can be configured.	

↘ Disabling IPv4 Routing

Command	**no ip routing**
Parameter Description	N/A
Defaults	By default, IPv4 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 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.

↘ Disabling IPv6 Routing

Command	**no ipv6 unicast-routing**
Parameter Description	N/A
Defaults	By default, IPv6 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 routing. If the device functions only as a bridge or a VoIP gateway, the device does not need to use the IPv6 routing function of the RGOS software. In this case, you can disable the IPv6 routing function of the RGOS software.

Verification

Run the **show running-config** command to display the configuration file and verify that the preceding configuration commands exist.

1.5 Monitoring

Clearing

Description	Command

Clears the route cache.	**clear ip route** { ***** **|** *network* [*netmask*] }

Displaying

Description	Command
Displays the IPv4 routing table.	**show ip route**
Displays the statistical information about IPv4 routing table.	**show ip route summary** [**all**]
Displays the IPv6 routing table.	**show ipv6 route**
Displays the statistical information about IPv6 routing table.	**show ipv6 route summary** [**all**]

Debugging

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

Description	Command
Debugs IPv4 route management.	**debug nsm kernel ucast- v4**
Debugs IPv6 route management.	**debug nsm kernel ucast-v6**
Debugs default network management.	**debug nsm kernel default-network**
Debugs internal events of route 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**

Configuring Multicast

1. Configuring IGMP Snooping
2. Configuring IPv4 Multicast Route Management

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.

Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

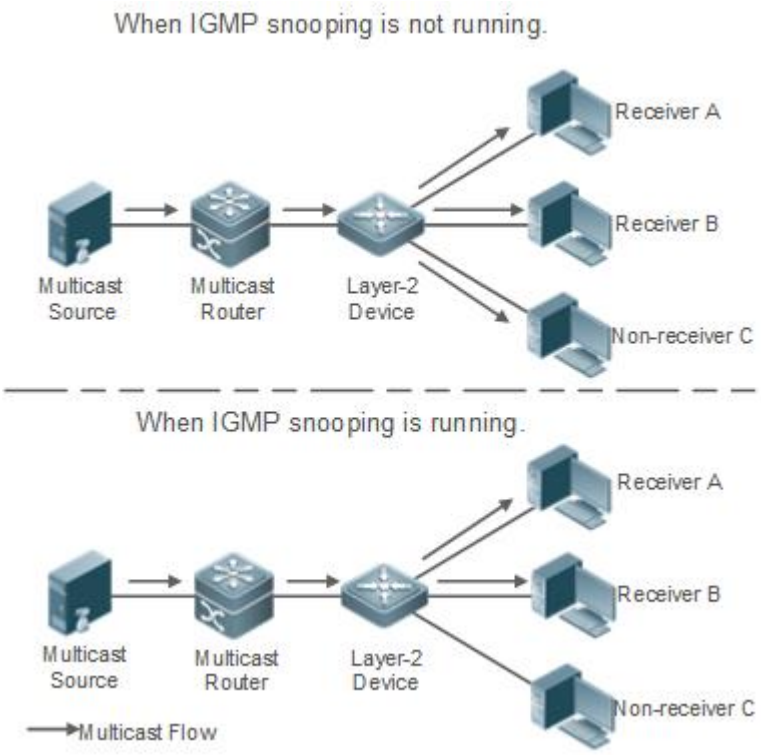
1.2 Applications

Application	Description
Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Multicast-to-Unicast Conversion	Implements transmission of multicast packets between the AP and STAs in unicast mode.

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 profile will no longer be broadcast within the VLAN but transmitted to designated receivers.
- Figure 1-1 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



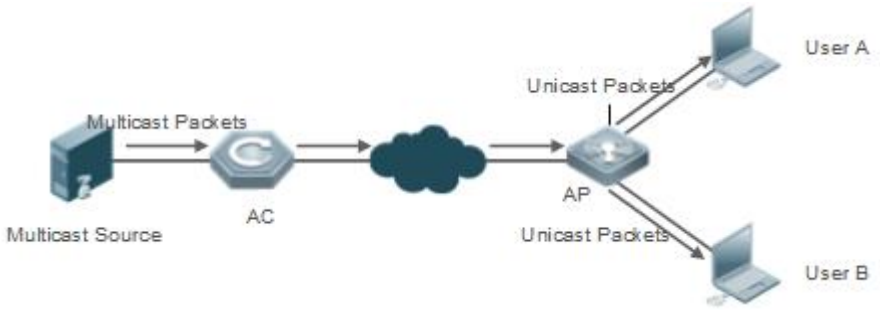
Deployment

- Configure basic IGMP snooping functions.

1.2.2 Multicast-to-Unicast Conversion

Scenario

- When multicast-to-unicast conversion is not configured, packets are transmitted from the AP to STAs in multicast mode. There is no acknowledgement and retransmission mechanism for multicast packets in wireless networks. As a result, severe packet loss occurs, which affect experience of wireless multicast services in video on demand and other applications. Wireless multicast packets between the AP and STAs can be configured to be transmitted in multicast-to-unicast conversion mode in order to reduce the packet loss rate and enhance user experience.
- Figure 1-2 Multicast-to-Unicast Conversion



Deployment

- Configure the multicast-to-unicast conversion function.

The function is available only in wireless multicast scenarios.

1.3 Features

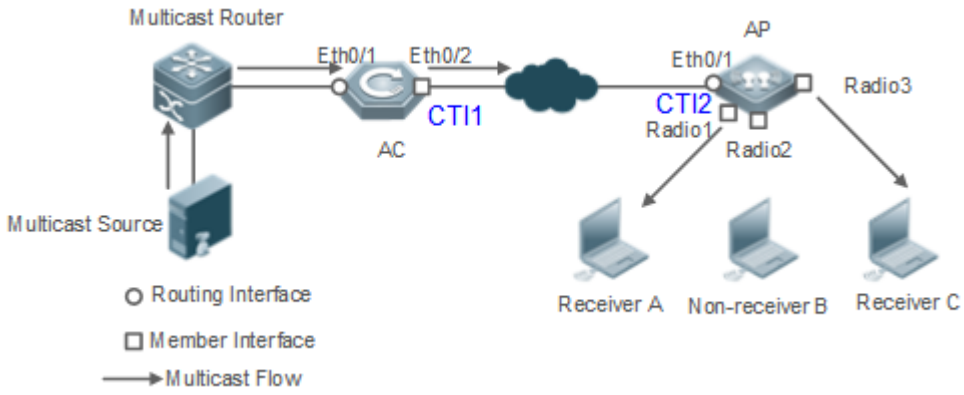
Basic Concepts

Multicast Router Ports and Member Ports

IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

The device running IGMP snooping identifies the ports within the VLAN as a multicast router port or member port so as to manage and control the forwarding of IP multicast traffic within the VLAN.

Figure 1-3 Two Types of Ports in Wireless Environment



- Multicast router port: When the AC receives the PIM Hello or IGMP Query packet from the upstream multicast router (Layer-3 multicast device), the multicast router port Ethq/1 forms. When the AP receives the PIM Hello or IGMP Query packet forwarded by the AC, the multicast router port CTI2 also forms.
- Member port: also called listener port, that is, the port on a device for connecting to a multicast member. When Ports Radio1 and Radio3 on the AP receive Report packets from a wireless user receiver, they learn the wireless port as a member port. When the virtual interface CTI1 receives Report packets forwarded by the AP, it also learns the relevant wireless port as a 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), profile 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.

```
Hostname# 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)
    caPWAP-Tunnel 0/1(D)     // CAPWAP tunnel
(*, 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)

(*,239.1.1.1, 1):    //(any source address, with the group address of 239.1.1.1 and VLAN ID of 1)
VLAN(1) 1 OPORTS:
    dot11radio 1/0.1 (D)    //wireless interface
```

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.
IGMP Querier	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.
Multicast-to-Unicast Conversion	Implements transmission of multicast packets between the AP and STAs in unicast mode.
Optimizing the Multicast Wireless Environment Configuration	Ignores port timer resetting for query packets.

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

When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a profile, it will also send a report.

By default, IGMP Snooping is capable of processing IGMPv1 and IGMPv2 packets. For IGMPv3 Report packets, it processes profile 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 profile will be forwarded.
- If the port on which Report packets are received is a dynamic member port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.
- If the port on which Report packets are received is not a dynamic member port, use it as a dynamic member port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.

Leave Packets

If a host requests to leave a profile, it will send a Leave packet.

When the device running IGMP snooping receives the Leave packets, it performs the following operations within the VLAN:

- Forward the leave packets from all the router ports.
- If the port on which leave packets are received is a dynamic member port and the Leave function is enabled, the port will be immediately deleted from the IGMP snooping forwarding entry of the designated profile and will no longer be used as the dynamic member port.
- If the port on which the leave packets are received is a dynamic member port and the Leave function is disabled, the port state should be maintained.

Related Configuration

Configuring a Static Router Port

Run the **ip igmp snooping vlan mrouter interface** command to configure a static router port.

Configuring a Static Member Port

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

Enabling Report Suppression

Report suppression is disabled by default.

Run the **ip igmp snooping suppression enable** command to enable report suppression.

After report suppression is enabled, in one IGMP query cycle, only the first Report packet received by each profile will be forwarded. The source media access control (MAC) address of the forwarded report will be changed to the MAC address of the device.

Enabling Immediate Leave

Immediate leave is disabled by default.

Run the **ip igmp snooping fast-leave enable** command to enable immediate leave.

Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a query packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time carried by the query packet.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

1.3.2 IGMP Snooping Working Modes

A device running in the IVGL mode of IGMP snooping can provide independent 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.

Related Configuration

Enabling IGMP Snooping and Selecting a Working Mode

IGMP snooping is disabled by default.

Run the **ip igmp snooping** command to enable IGMP snooping in IVGL mode.

1.3.3 IGMP Querier

On a network with a Layer-3 multicast device, the Layer-3 multicast device acts as an IGMP querier. In this case, a Layer-2 device needs only to listen to IGMP packets to establish and maintain the forwarding entry, realizing Layer-2 multicast.

On a network without a Layer-3 multicast device, the Layer-2 multicast device must be configured with the IGMP querier function so that the device can listen to IGMP packets. In this case, a Layer-2 device needs to act as an IGMP querier as well as listen to IGMP packets to establish and maintain the forwarding entry to realize Layer-2 multicast.

Working Principle

A Layer-2 device acts as an IGMP querier to periodically send IGMP Query packets, listen to and maintain the IGMP Report packets replied by a user, and create a Layer-2 multicast forwarding entry. You can adjust relevant parameters of the Query packets sent by the IGMP querier through configuration.

When the device receives a Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP) packet, it considers that a multicast router, which will act as an IGMP querier, exists on the network and disables the querier function. In this way, IGMP routing will not be affected.

When the device receives the IGMP Query packets from other devices, it will compete with other devices for the IGMP querier.

↘ Enabling the Querier Function

You can enable the querier for a specific VLAN or all VLANs.

Only when the global querier function is enabled can the queriers for specific VLANs take effect.

↘ Specifying the IGMP Version for a Querier

The version of IGMP used for sending Query packets can be configured as IGMPv1, IGMPv2, or IGMPv3.

↘ 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** *vid* **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** *vid* **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** *vid* **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** *vid* **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** *vid* **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** *vid* **querier timer expiry** command to configure the aging time of queriers on specific VLANs.

1.3.4 Multicast-to-Unicast Conversion

The multicast-to-unicast conversion function is available only in wireless environment. After the function is configured on a wireless device, multicast packets between an AP and STAs are transmitted in unicast mode. The multicast-to-unicast conversion function runs on the AP.

Working Principle

The following describes the working principle of multicast-to-unicast conversion from several scenarios in wireless environment.

In fat AP mode, IGMP Snooping needs to learn and track user information. After multicast-to-unicast conversion is configured, the wireless multicast fast forwarding module queries the users who need multicast-to-unicast conversion through the interface provided by the multicast-to-unicast conversion module, and replaces the destination MAC addresses in multicast packets of the users with the MAC addresses of STAs, and destination IP addresses with IP addresses of the STAs, and then forwards the multicast packets in unicast mode.

In fit AP centralized forwarding mode, an AC, according to recorded user information, queries the WLAN ID and RADIO ID of an STA for packets, conducts CAPWAP encapsulation on the packets, and then sends the packets to an AP. If the multicast-to-unicast conversion is enabled, packets sent to the AP are delivered to the wireless multicast fast forwarding module, which queries the interface of the multicast-to-unicast conversion module to learn about the users who need multicast-to-unicast conversion. Then, the AP transmits multicast packets in unicast mode.

In fit AP local forwarding mode, after packets are forwarded to an AP, if multicast-to-unicast conversion is enabled, the AP delivers the packets to the wireless multicast fast forwarding module, which transmit multicasts the packets in unicast mode.

Related Configuration

↘ Enabling the Global Multicast Function

By default, the global multicast function is disabled.

Run the **no ip multicast wlan** command to restore default configuration. After global multicast is disabled, an AC directly discards the received multicast packets.

↘ Enabling Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is disabled.

Run the **ip igmp snooping mcast-to-unicast enable** command to enable multicast-to-unicast conversion.

Run the **no ip igmp snooping mcast-to-unicast enable** command to disable multicast-to-unicast conversion.

↘ Configuring the Multicast Range for Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is available to all multicast profiles.

Run the **igmp snooping mcast-to-unicast group-range** command to configure the profile address range for multicast-to-unicast conversion.

Run the **no igmp snooping mcast-to-unicast group-range** command to restore the default configuration.

↘ Configuring the Maximum Number of Profiles That Are Allowed to Use Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion can be configured for a maximum of 64 multicast profiles.

Run the **igmp snooping mcast-to-unicast max-group** command to configure the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion.

Run the **no igmp snooping mcast-to-unicast max-group** command to restore the default configuration.

1.3.5 Optimizing the Multicast Wireless Environment Configuration

Ignoring port timer resetting for query packets refers to not resetting the port aging timer when a device receives query packets.

When multiple STAs are configured in a congested wireless network, after an AP sends out a query packet, the IGMP report packet responded by STAs may be discarded or the STAs fail to receive the query packet, and as a result, the AP fails to receive responses from the STAs. Traffic interruption may occur on the STAs. In this case, this function can be configured, in combination with aging time configuration of member ports, to ensure that an STA does not age within multiple query intervals. If an IGMP report packet from the STA is received within the query intervals, the port timer time is reset as the port aging time.

The configuration takes effect when query packets are received next time. A port timer that has been reset on a port will not be cancelled. The configuration prolongs aging time. Use it in appropriate scenarios.

The function is disabled by default.

Run the **igmp snooping ignore-query-timer** command to ignore the port aging timer resetting for query packets.

Run the **no igmp snooping ignore-query-timer** command to restore the default configuration.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic IGMP Snooping Functions (IVGL Mode)	⚠ Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL mode.	
	ip igmp snooping	Enables global IGMP snooping on a Fat AP.
	no ip igmp snooping vlan *num*	Disables IGMP snooping for a VLAN.
Configuring the Packet Processing	⚠ (Optional) It is used to adjust relevant configurations for processing protocol packets.	

	ip igmp snooping vlan *vid* **mrouter interface** *interface-type interface-number*	Configures a static router port.
	ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*	Configures a static member port.
	ip igmp snooping host-aging-time *time*	Configures the aging time of a dynamic member port on a Fat AP.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	ip igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet on a Fat AP.
	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.
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 *vid* **querier**	Enables the querier for a VLAN.
	ip igmp snooping querier version *num*	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan *vid* **querier version** *num*	Specifies the IGMP version for a querier of a VLAN.
	ip igmp snooping querier address *ip-address*	Configures the source IP address of queriers globally.
	ip igmp snooping vlan *vid* **querier address** *ip-address*	Configures the source IP address for a querier of a VLAN.
	ip igmp snooping querier query-interval *seconds*	Configures the query interval of queriers globally.
	ip igmp snooping vlan *vid* **querier query-interval** *seconds*	Configures the query interval for a querier of a VLAN.
	ip igmp snooping querier max-response-time *seconds*	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan *vid* **querier max-response-time** *seconds*	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry *seconds*	Configures the aging timer for queriers globally.
	ip igmp snooping vlan *vid* **querier timer expiry** *seconds*	Configures the aging timer for a querier of a VLAN.
Configuring Multicast-to-Unicast	**ip igmp snooping mcast-to-unicast enable**	Enables multicast-to-unicast conversion on an Fat AP.

Conversion	**ip igmp snooping mcast-to-unicast group-range *ip-address*** *ip-address*	Configures an AP's maximum multicast range for multicast-to-unicast conversion on a Fat AP.
	ip igmp snooping mcast-to-unicast max-group *number*	Configures an AP's maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion on a Fat AP.
Optimizing the Wireless Multicast Environment	**ip igmp snooping ignore-query-timer**	Configures the function of ignoring port aging timer resetting for query packets on a Fat AP.

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.

Configuration Steps

↘ Enabling Global IGMP Snooping in IVGL Mode

Mandatory.

After IGMP snooping is enabled globally, this function will be enabled for all VLANs.

↘ 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 on a Fat AP

Command	**ip igmp snooping**
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** *vid*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Only when global IGMP snooping is enabled can it be disabled on specified VLANs. In IVGL mode, you can disable IGMP snooping on any VLAN.

Displaying the IGMP Snooping Entry

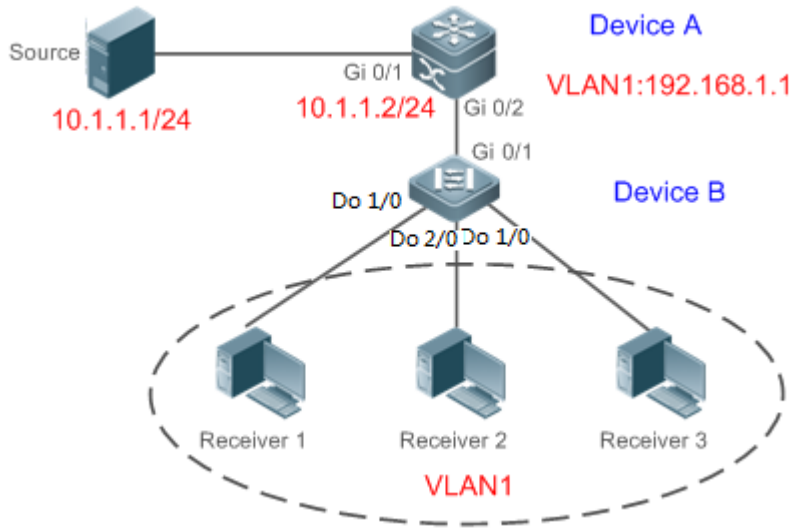
Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

Displaying the IGMP Snooping Working Mode

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL mode, the following information is displayed: IGMP Snooping running mode: IVGL

Configuration Example

Providing Layer-2 Multicast Services for the Subnet Hosts

Scenario Figure 1-4	
	A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1, Receiver 2, and Receiver 3 belong to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)# ip igmp snooping
Verification	Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G. ● Confirm that the packets (10.1.1.1 and 229.1.1.1) are received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the port (10.1.1.1, 229.1.1.1, 1) includes only Gi0/2. ● Check whether the IGMP snooping working mode is IVGL.
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(1) 2 OPORTS: 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 the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all profiles.
- Configure specified ports as the static member ports to receive the multicast traffic from specified profiles
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or profile to the router port within a query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network.
- Configure the immediate-leave function to delete a port from the entry of member ports when a leave packet is received by the port.
- Disable dynamic router port learning to disable the learning of any router port.
- Based on network load and configuration of a multicast device, you can adjust the aging time of a router port and member port as well as the maximum response time of a query packet.

Notes

- Only when basic IGMP snooping is configured can relevant configurations take effect.

Configuration Steps

Configuring a Static Router Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive all the multicast traffic within the VLAN.

Configuring a Static Member Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive specific multicast traffic within the VLAN.

Enabling Report Packet Suppression

- Optional.
- When there are numerous receivers to receive the packets from the same multicast profile, you can enable Report packets suppression to suppress the number of Report packets to be sent.

Enabling the Immediate-Leave Function

- Optional.
- When there is only one receiver on a port, you can enable Leave to speed up the convergence of protocol upon leave.

Configuring the Aging Time of a Dynamic Member Port

- Optional.
- You can configure the aging time based on network load

Configuring the Maximum Response Time of a Query Packet

- Optional.
- You can configure the maximum response time based on network load.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

Configuring a Static Router Port

Command	**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	the configurations for the static router ports within all the VLANs can take effect.

Configuring a Static Member Port

Command	**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *group-address*: Indicates a profile address. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

Enabling Report Packet Suppression

Command	**ip igmp snooping suppression enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, 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	When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address. 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.

Configuring the Aging Time of a Dynamic Member Port

Command	**ip igmp snooping host-aging-time** *seconds*
Parameter Description	*seconds*: Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	The aging time of a dynamic member port indicates the time when a device port receives the IGMP join packet sent from host for subscribing to an IP multicast profile. When the IGMP join packet is received, the aging time of the dynamic member port will be reset. The value of the timer time is host-aging-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. After the aging time is configured, the aging time of following received IGMP join packets will be host-aging-time. This configuration takes effect after the next IGMP join packet is received, and the timer of the port in use will not be refreshed.

Configuring the Maximum Response Time of a Query Packet

Command	**ip igmp snooping query-max-response-time** *seconds*
Parameter Description	*seconds*: Indicates the maximum response time.
Command Mode	Global configuration mode
Usage Guide	When an IGMP general Query packet is received, the multicast device will reset the aging time of all the dynamic member ports, which is query-max-response-time.

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	If the router port is successfully configured, an "S" will be displayed in the port information. Hostname#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)

Displaying the Information of Dynamic Router Port Learning

Command	**show ip igmp snooping**
Parameter Description	N/A

Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time and learning status of the dynamic router port. Dynamic Mroute Aging Time : 300(Seconds) Multicast router learning mode: pim-dvmrp

Displaying the Information of a Member Port

Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the member port is successfully configured, an "S" will be displayed in the port information. Hostname#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/1(S

Displaying Other Parameters

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave. IGMP Fast-Leave: Enable IGMP Report suppress: Enable Query Max Response Time: 20(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

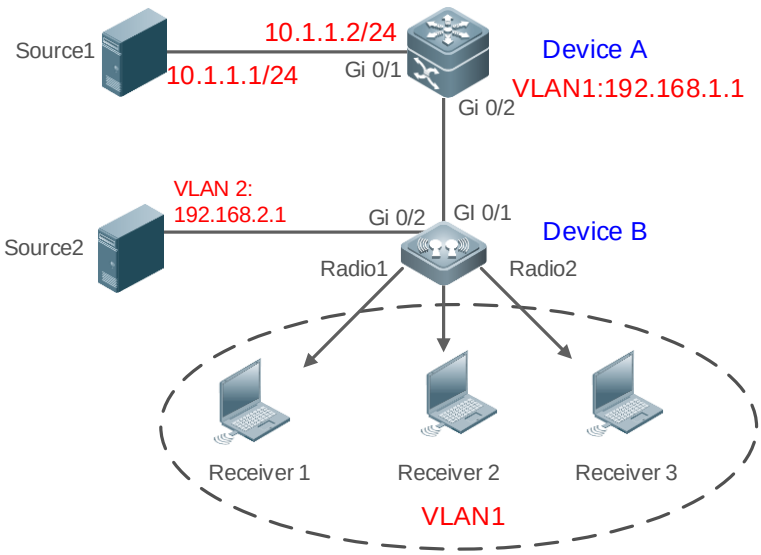
Configuration Example

Configuring a Static Router Port and Static Member Port

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.

	Hostname# configure terminal Hostname(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/1 Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface gigabitethernet 0/1 Hostname(config)# end
Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.
	Hostname#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S) Hostname#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/1(SM)

Enabling Report Packet Suppression

Scenario Figure 1-5	
	A is the multicast router and is connected directly to multicast Source 1 and Source 2. B is a Layer-2 device and is connected directly to the user host. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface

	(Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode. ● Enable Report packets suppression on B.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping B(config)# ip igmp snooping suppression enable
Verification	Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.
B	B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

↘ Configuring Other Parameters

Configuration Steps	● Configure basic IGMP snooping functions. ● Enable Immediate-leave function. ● Disable router port learning. ● Configuring the aging time of a member port. ● Configure the response time of a Query packet.
	Hostname# configure terminal Hostname(config)# ip igmp snooping fast-leave enable Hostname(config)# no ip igmp snooping mrouter learn pim-dvmrp Hostname(config)#ip igmp snooping host-aging-time 100 Hostname(config)#ip igmp snooping query-max-response-time 60 Hostname(config)# end
Verification	Run the **show ip igmp snooping** command to check whether the configuration is successful.

	Hostname#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Host Aging Time : 100(Seconds)

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

1.4.3 Configuring an IGMP Querier

Configuration Effect

- Configure the device as an IGMP querier, which will send IGMP Query packets periodically and collect user demanding information.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↘ Enabling the Querier Function

- (Optional) Enable IGMP querier function globally or for a specified VLAN.
- (Optional) Disable the IGMP querier function for a specified VLAN.

↘ Configuring the Source IP Address of a Querier

- (Optional) You can configure the source IP address of a Query packet sent by the querier based on VLANs.
- After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect.

↘ Configuring the Maximum Response Time of a Query Packet

- (Optional) Adjust the maximum response time carried by an IGMP Query packet. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1.

Configuring the Query Interval of a Querier

- (Optional) Adjust the interval of the IGMP querier for sending query packets.

Configuring the Aging Timer of a Querier

- (Optional) Configure the aging timer of other IGMP queriers on the network.

Specifying the IGMP Version for a Querier

- (Optional) Specify the IGMP version for a querier (IGMPv2 by default).

Verification

- Run the **show ip igmp snooping querier detail** command to check whether the configuration takes effect.

Related Commands

Enabling the IGMP Querier Function

Command	**ip igmp snooping** [**vlan** *vid*] **querier**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	IGMP querier for a specified VLAN will take effect only after global IGMP querier is enabled. If global IGMP querier is disabled, IGMP querier for all the VLANs will be disabled.

Configuring the Source IP Address of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *a.b.c.d*: Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect. If the source IP address is specified by a VLAN, the address will be used preferentially.

Configuring the Maximum Response Time of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier max-response-time** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the maximum response time. in the unit of seconds. The value ranges from 1 to 25.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Query Interval of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier query-interval** *seconds*

Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the query interval in the unit of seconds. The value ranges from 1 to 18,000.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Aging Timer of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier timer expiry** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the timeout time in the unit of seconds. The value ranges from 60 to 300.
Command Mode	Global configuration mode
Usage Guide	A device may fail to be elected as the querier even when its querier function is enabled. If a device that fails to be elected does not receive the Query packet sent by the querier in the aging time, the querier in use is considered as expired, and a new round of election will be raised. If the aging time is specified by a VLAN, the value will be used preferentially.

Specifying the IGMP Version for a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier version 1**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A querier can be run in IGMPv1 and IGMPv2 (IGMPv2 by default). You can also run a command to configure the version to IGMPv1. If the IGMP version for a querier is specified by a VLAN, the version will be used preferentially.

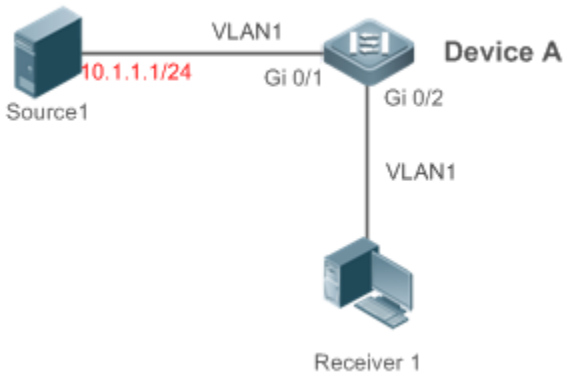
Displaying the IGMP Querier Configuration

Command	**show ip igmp snooping querier detail**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed. Hostname(config)#show ip igmp snooping querier detail Vlan IP Address IGMP Version Port ---------- Global IGMP switch querier status ---------- admin state : Enable admin version : 2 source IP address : 1.1.1.1 query-interval (sec) : 60

	max-response-time (sec) : 10 querier-timeout (sec) : 125 Vlan 1: IGMP switch querier status ---------- admin state : Disable admin version : 2 source IP address : 1.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 operational state : Disable operational version : 2

Configuration Example

↘ Enabling the IGMP Querier Function

Scenario Figure 1-6	
	In the scenario without Layer-3 multicast equipment, the multicast traffic can be forwarded only on the Layer-2 network. A acts as a Layer-2 device to connect to the multicast source and receiver.
Configuration Steps	● Enable global IGMP snooping on A in IVGL mode. ● Enable IGMP querier for VLAN 1 on A.
A	A(config)#ip igmp snooping A(config)#ip igmp snooping querier A(config)#ip igmp snooping querier address 10.1.1.1 A(config)#ip igmp snooping vlan 1 querier
Verification	Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.
A	A(config)#show ip igmp snooping querier Vlan IP Address IGMP Version Port ---------- 1 10.1.1.1 2 switch

	A(config)#show ip igmp snooping querier vlan 1 Vlan 1: IGMP switch querier status ---------- elected querier is 10.1.1.1 (this switch querier) ---------- admin state : Enable admin version : 2 source IP address : 10.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 operational state : Querier operational version : 2

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

1.4.4 Configuring Multicast-to-Unicast Conversion

Configuration Effect

- Enable the multicast-to-unicast conversion on the AP, which transmits multicast packets to STAs in unicast mode.

Notes

- IGMP Snooping basic functions must be configured.

Configuration Steps

↘ Enabling Global Multicast

- (Mandatory) Enable global multicast in global mode.
- If global multicast is disabled in global mode, a wireless device directly discards received packets.

↘ Enabling Multicast-to-Unicast Conversion

- (Optional) Configure whether to enable multicast-to-unicast conversion. After multicast-to-unicast conversion is enabled, after packets reach the AP, the AP judges the multicast packets that need to be transmitted in unicast mode and transmits such packets in unicast mode.

↘ Configuring the Multicast Range for Multicast-to-Unicast Conversion

- (Optional) Multicast-to-unicast conversion is available to all multicast groups by default. A multicast range can be configured to allow multicast packets to be transmitted in unicast mode, so as to utilize AP resources to the maximum extent.

Configuring the Maximum Number of Multicast Profiles that Are Allowed to Use Multicast-to-Unicast Conversion

- (Optional) The maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion can be adjusted.
- It is used in combination with the multicast range of multicast-to-unicast conversion.

Verification

- Run the show ip igmp snooping command to check whether the configuration takes effect.

Related Commands

Configuring Global Multicast

Command	**ip multicast wlan**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If global multicast is enabled, multicast packets are processed only after they reach the AC. If global multicast is disabled, the AC directly discards the received multicast packets.

Configuring Multicast-to-Unicast Conversion

Command	**ip igmp snooping mcast-to-unicast enable**
Parameter Description	N/A
Command Mode	ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	After multicast-to-unicast conversion is enabled, when multicast packets reach the AP, the AP judges the multicast packets that need to be transmitted in unicast mode according to the multicast-to-unicast conversion policy.

Configuring the Maximum Multicast Range for Multicast-to-Unicast Conversion

Command	**ip igmp snooping mcast-to-unicast group-range** *ip-addr ip-addr*
Parameter Description	*ip-addr:* Indicates the multicast profile range. The value must be valid multicast addresses and ranges from 224.0.1.0 to 239.255.255.255.
Command Mode	Ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	If the multicast range of multicast-to-unicast conversion is not configured, multicast-to-unicast conversion is available to all multicast profiles by default.

Configuring the Maximum Number of Multicast Profiles That Are Allowed to Use Multicast-to-Unicast Conversion

Command	**ip igmp snooping mcast-to-unicast max-group** *number*
Parameter	number: Indicates the maximum number of multicast profiles that are allowed to use

Description	multicast-to-unicast conversion. The value ranges from 1 to 64. The default value is 64.
Command Mode	global configuration mode on the fat AP
Usage Guide	It can be used in combination with the maximum multicast range of multicast-to-unicast conversion so as to properly allocate bandwidth and effectively control AP resources.

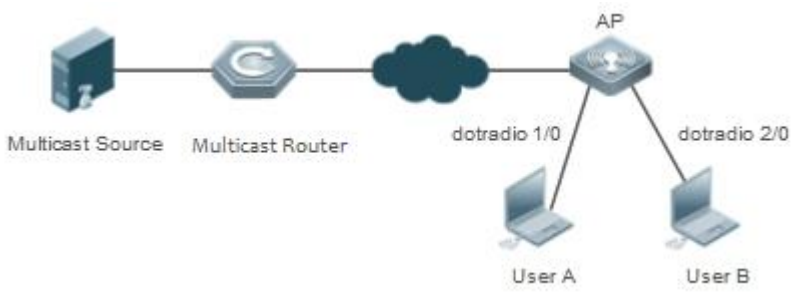
Displaying Multicast-to-Unicast Conversion Configuration

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	If multicast-to-unicast conversion is configured successfully, the following information is displayed: Hostname(config)#sh ip igmp snooping WLAN Multicast: Enable IGMP Snooping running mode: IVGL IGMP Snooping M2U-Forward: Enable IGMP Snooping Support M2U Max-Group Num: 64 IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64 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)

Configuration Example

The following configuration example describes only configurations related to IGMP Snooping.

Enabling the IGMP Querier

Scenario Figure 1-7	

	Multicast streams only need to be forwarded at Layer 2 in network deployment and there is no device supporting the Layer-3 multicast function in the network. User A and User B are multicast receivers.
Configuration Steps	● Enable IGMP Snooping on the AP ● Enable global multicast on the AP ● Enable IGMP Snooping in global configuration mode. ● Enable multicast-to-unicast conversion in global configuration mode. ● Configure the maximum multicast range for multicast-to-unicast conversion global configuration mode.. ● Configure the maximum number of multicast profiles that are allowed to support multicast-to-unicast conversion in global configuration mode..
A	A(config)#ip igmp snooping ivgl A(config)#ip multicast wlan A(config)#ip igmp snooping A(config)#ip igmp snooping mcast-to-unicast enable A(config)#ip igmp snooping mcast-to-unicast group-range 233.1.1.1 233.255.255.255 A(config)#ip igmp snooping mcast-to-unicast max-group 10
Verification	Run the **show ip igmp snooping** command to check whether the configuration takes effect.
A	A(config)# sh ip igmp snooping WLAN Multicast: Enable IGMP Snooping running mode: IVGL IGMP Snooping M2U-Forward: Enable IGMP Snooping Support M2U Max-Group Num: 64 IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64 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)

Common Errors

- Multicast packets are not processed because global multicast is not configured.

1.4.5 Optimizing the Wireless Multicast Environment

Configuration Effect

- Configure the function of ignoring port timer resetting for query packets on the wireless device.

Notes

- IGMP Snooping basic functions must be configured.

Configuration Steps

↘ Configuring the Function of Ignoring Port Aging Timer Resetting for Query Packets

- (Optional) Configure the function of ignoring port aging timer resetting for query packets so that the port does not age within multiple query intervals.

Verification

- Run the **show ip igmp snooping** command to check whether the configuration takes effect.

Related Commands

↘ Configuring the Function of Ignoring Port Aging Timer Resetting for Query Packets

Command	**ip igmp snooping ignore-query-timer**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the function of ignoring port aging timer for query packets is configured, the port does not age within multiple query intervals. When the port receives a Report request, the port aging timer resets.

1.5 Monitoring

Clearing

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

Description	**Command**
Clears the dynamic router ports and member ports.	**clear ip igmp snooping gda-table**

Displaying

Description	**Command**
Displays basic IGMP snooping configurations.	**show ip igmp snooping** [**vlan** *vlan-id*]
Displays the router ports.	**show ip igmp snooping mrouter**
Displays the IGMP snooping entries.	**show ip igmp snooping gda-table**
Displays the IGMP querier.	**show ip igmp snooping querier** [**detail**]
Displays user information.	**show ip igmp snooping user-info**

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**

1 Configuring IPv4 Multicast Route Management

1.1 Overview

IP multicasting is abstracted hardware multicasting and an extended multicast routing protocol on the standard IP network layer.

In traditional IP transmission, only one host can send packets to a single host (unicast communication) or all hosts (broadcast communication). However, the multicast technology provides the third choice: a host can send packets to certain specified hosts.

IP multicasting is applicable to one-to-many multimedia applications.

1.2 Features

Overview

Feature	Description
Configuring Forced Forwarding of Multicast Packets by Software	IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

1.2.1 Configuring Forced Forwarding of Multicast Packets by Software

IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

Working Principle

After configuring this function, all IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

Related Configuration

↘ **Configuring Forced Forwarding of CPU-destined IPv4 Multicast Data Packets by Software**

This function is disabled by default.

Run **msf force-forwarding** to enable IPv4 multicast data packets destined for the CPU to be forcedly forwarded by software.

1.3 Configuration

Configuration	Description and Command

Configuring Forced Forwarding of Multicast Packets by Software	**msf force-forwarding**	Configures forced forwarding of multicast packets by software.

1.3.1 Configuring Forced Forwarding of Multicast Packets by Software

Configuration Effect

- After configuring this function, all IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Configure forced forwarding of multicast packets by software on each device unless otherwise specified.

Verification

Run **show running-config** to check whether forced forwarding of multicast packets by software is configured.

Related Commands

↘ **Configuring Forced Forwarding of Multicast Packets by Software**

Command	**msf force-forwarding**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Only configuration related to IP multicasting is described.

↘ **Creating the IP Multicast Service on the IPv4 Network and Configuring Forced Forwarding of Multicast Packets by Software**

Scenario	Basic environment for the IP multicast service

Figure 1-1	
Configuration Steps	● Configure the basic functions of IP multicasting. ● Configure forced forwarding of multicast packets by software.
A	A# configure terminal A(config)#msf force-forwarding
Verification	Run **show running-config** to check whether forced forwarding of multicast packets by software is configured.
A	A# show running-config ... msf force-forwarding ...

1.4 Monitoring

Displaying

Description	Command
Displays the IPv4 multi-layer multicast forwarding table.	**show msf msc**
Displays IPv4 multicast non-stop forwarding configurations.	**show msf nsf**

Debugging

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

Description	Command
Debugs the processing of IPv4 multi-layer multicast packet forwarding.	**debug msf forwarding**
Debugs the operation on multi-layer multicast forwarding entries on an IPv4 network.	**debug msf mfc**
Debugs the bottom-layer hardware processing of IPv4 multi-layer multicast packet forwarding.	**debug msf ssp**
Debugs the invocation of API interfaces provided by IPv4 multi-layer multicast forwarding.	**debug msf api**
Debugs the processing of multi-layer multicast forwarding events on an IPv4 network.	**debug msf event**

Configuring AP Management

1. Configuring CAPWAP
2. Configuring iBeacon

1 Configuring CAPWAP

1.1 Overview

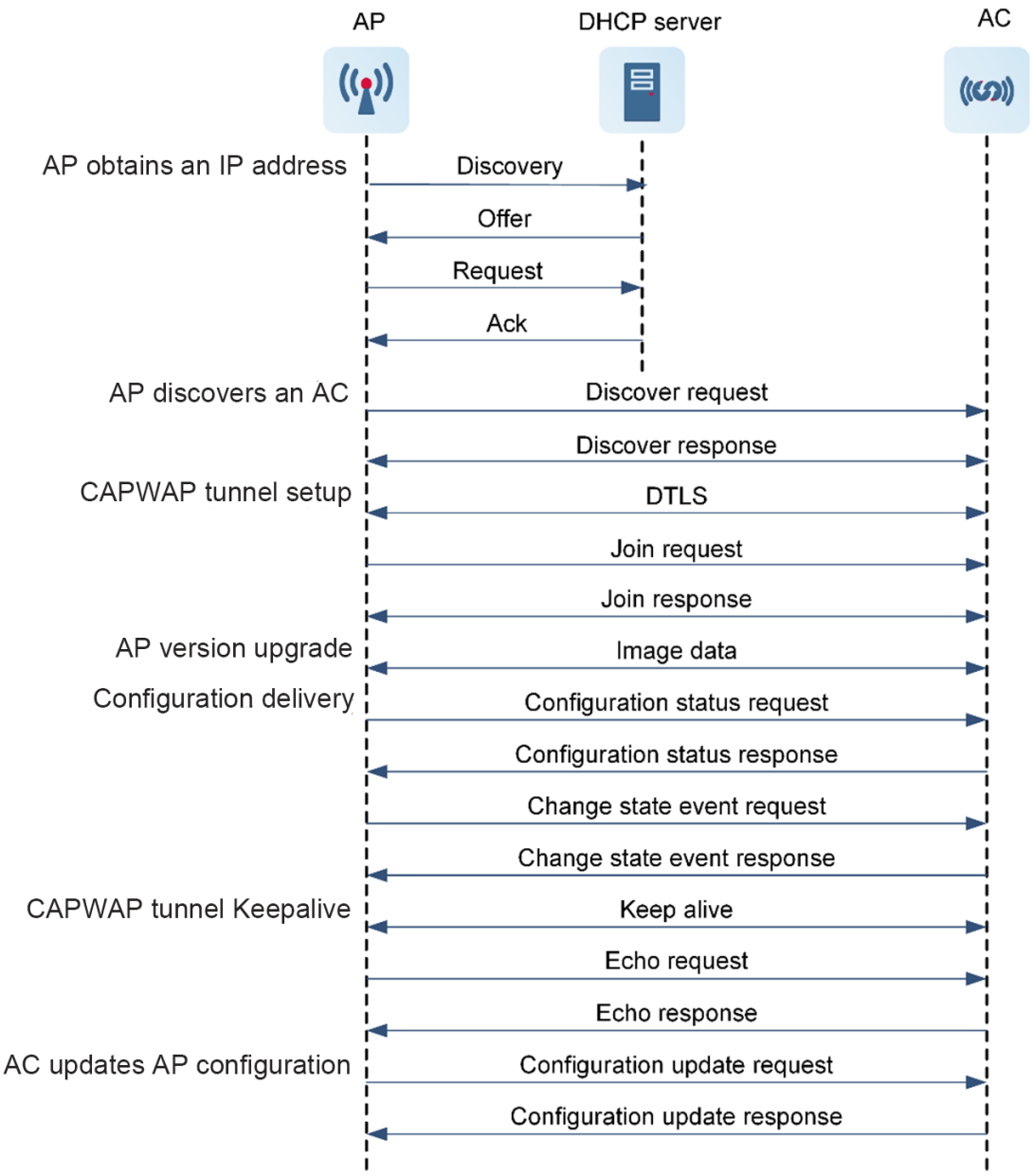
On a wireless local area network (WLAN), the network in which an access controller (AC) manages all access points (APs) is called a fit AP wireless network. On such a network, APs provide wireless access services for wireless stations and bridge communication between the WLAN and traditional wired network. The AC communicates with APs through the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. CAPWAP tunnels are established through negotiation between the AC and APs on the Layer 2 network or across the Layer 3 network based on the encapsulation technology and transmission mechanism of CAPWAP to achieve data interaction

1.1.1 Working Principle

Before an AC manages APs on a fit AP network, an AP must obtain an IP address and sends an AC Discover request with the IP address as the source address. After the AP discovers potential ACs, it selects the optimal AC from the potential ACs to establish a CAPWAP tunnel.

Through the CAPWAP channel, the AC delivers service configuration to APs and manages them uniformly. Service data of users connected to the APs is encapsulated and then uploaded to the AC for forwarding. Figure 1-1 shows the working procedure of the CAPWAP tunnel. This procedure includes AC discovery by the AP, CAPWAP tunnel establishment, AP version upgrade, configuration delivery and update, and CAPWAP tunnel maintenance.

Figure 1-1 CAPWAP Tunnel Establishment



1. The AP obtains an IP address.

The management IP address of an AP can be an IPv4 or IPv6 address, which allows you to establish an IPv4 or IPv6 CAPWAP tunnel. An AP can dynamically obtain an IP address through Dynamic Host Configuration Protocol (DHCP) or use a manually configured IP address. The DHCP mode is recommended.

- DHCP-based dynamic allocation: After a DHCP server is deployed, the AP is powered on and serves as a DHCP client by default. The AP then proactively sends a DHCP Request message to the DHCP server, as shown in Figure 1-1.
- Manual configuration: A network administrator logs in to the AP to manually configure a static IP address.

2. The AP discovers an AC.

An AP can discover ACs of IPv4 and IPv6 protocol stacks. The two discovery processes are similar. In Figure 1-1, the AP broadcasts a Discover request and waits for the ACs' response. Upon receiving the Discover request, the ACs determine whether to allow the AP's access based on the access policy. If so, the ACs send Discover responses to the AP. If not, the ACs do not respond to the AP. Upon receiving multiple Discover responses from ACs, the AP selects the optimal AC based on the AC priority policy and starts to establish a CAPWAP tunnel. The AC priority policy includes the priority of AC discovery modes, AC load, AC's IP address, and other factors.

The AP discovers ACs in dynamic discovery or static configuration mode. Dynamic discovery is recommended to reduce manual configuration.

- Static configuration

In this mode, the static AC address or AC address list is manually pre-configured. After obtaining the IP address, the AP unicasts a Discover request to all pre-configured ACs and selects the optimal AC from the received Discover responses to join the AC. Typically, a statically configured AC has the highest priority.

- Dynamic discovery

An AC can be dynamically discovered in unicast, multicast, or broadcast mode. The unicast mode falls into the DHCP mode and Domain Name Server (DNS) mode. In fit AP mode, ACs and the AP reside on different network segments. Therefore, the ACs cannot be discovered in broadcast or multicast mode. The DHCP mode is recommended in this case.

  - DHCP mode

    An AP obtains an IP address through DHCP, which means that the AP discovers ACs in DHCP mode. On an IPv4 network, the DHCP server is configured with Option 138 or Option 43 that defines the AC's address. The DHCP server sends a DHCP ACK message carrying the AC's address to the AP. On an IPv6 network, the DHCP server is configured with Option 52 that defines the AC's address. Then the DHCP server sends a DHCP ACK message carrying the AC's address to the AP. After parsing the Option field, the AP discovers the AC, unicasts a Discover request to the AC, and waits for the AC's response.

  - DNS mode

    The AC's domain name and the address of the DNS server that parses this domain name are configured on the DHCP server. When the AP is dynamically obtaining an IP address, the DHCP ACK message that carries the preceding information is sent to the AP. Upon receiving the AC's domain name and the address of the DNS server, the AP sends a parsing request to the DNS server, discovers the AC based on the DNS response, unicasts a Discover request to the AC, and waits for the AC's response.

  - Broadcast or multicast mode

The broadcast or multicast mode applies to the scenario where APs and the AC are located on the Layer 2 network of the same network segment. The AP broadcasts or multicasts a Discover request to discover potential ACs.

3. The AP applies for joining an AC.

CAPWAP tunnel establishment includes setup of control and data channels. The control channel is used for transmitting control packets between the AC and APs (for example, the AC configures the APs uniformly and advertises messages to the APs). The data channel is used for forwarding the packets to the AC after service packets received by the APs are encapsulated into CAPWAP packets.

The AP processes a received AC Discover response with the following methods:

- If the packet carries the encryption ID, the AP negotiates and establishes a datagram transport layer security (DTLS) channel with the AC and sends a Join request in ciphertext mode to join the AC.
- If the packet does not carry the encryption ID, the Join request in cleartext mode is sent.

The Join request sent by the AP includes AP version information. Upon receiving the information, the AC verifies the validity of the AP, including the AP name, MAC address of the AP, AP certificate, and key, and returns a Join response to the AP. Based on the Join response, the AP determines whether it needs version upgrade. If not, the AP sends a Configuration status request to the AC. Upon receiving the request, the AC delivers the current configuration of the AP to the AP. The AP updates the CAPWAP tunnel state as running. If so, the AP upgrades its version.

4. The AP version is upgraded.

Based on parameters in the received Join response, if the AP determines that the local software version is inconsistent with that specified by the AC, the AP downloads the latest software version from the AC to upgrade the local software. After the AP is upgraded, it obtains an IP address again, discovers and joins the optimal AC, and updates the CAPWAP tunnel state as running.

The AC supports three AP upgrade modes. The self-adaptive version upgrade mode is recommended to reduce maintenance load.

- Self-adaptive version upgrade

  The AC automatically identifies an applicable software version for APs based on AP upgrade files and upgrades the software of the APs to the same version.

- Specified AP series version upgrade

  APs of the same series sharing one version file are upgraded uniformly.

- Specified single AP version upgrade

  The upgrade version of a single AP is manually specified.

5. The CAPWAP tunnel retains connected.

After channels are established between the AP and AC, the AP initiates an Echo request every 30s through UDP port 5246 with the AC to detect the connection state of a control channel.

After channels are established between the AP and AC, the AP sends a Keepalive packet through UDP port 5247 to detect the connection state of a data channel.

The CAPWAP tunnel can retain connected only when AC responses are received through both the control channel and data channel.

Protocols and Standards

- RFC 5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC 5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
- RFC 5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.2 Configuration Task Summary

CAPWAP configuration includes the following tasks:

- Configuring AP Connection Parameters (the following configuration tasks are optional, and you can select them as required)
  - Configuring an AP to Discover an AC in Static Configuration Mode
  - Configuring a Static IP Address for an AP Interface
  - Configuring a Working Mode of the AP

1.3 Configuring AP Connection Parameters

1.3.1 Overview

Configuring AP connection parameters includes manually configuring a static IP address for an AP interface and configuring a policy for an AP to discover an AC. You can log in to the AP to modify these parameters based on network deployment requirements.

1.3.2 Configuration Tasks

Configure AP connection parameters. The following tasks are optional. Select them as required.

- Configuring an AP to Discover an AC in Static Configuration Mode
- Configuring a Static IP Address for an AP Interface

1.3.3 Configuring an AP to Discover an AC in Static Configuration Mode

Overview

In this mode, you can manually pre-configure one static AC address or an AC address list. After obtaining the IP address, the AP unicasts a Discover request to all pre-configured ACs and selects the optimal AC from the received Discover responses to join the AC. Typically, a statically configured AC has the highest priority. No static AC IPv6 address is configured by default.

Configuration Steps

1. Enter the privileged EXEC mode.

```
enable
```

2. Enter the global configuration mode.

```
configure terminal
```

3. Configure a static AC address.

IPv4 network:

```
acip ipv4 ac-ipv4-address&<1-6>
```

Configure the static AC IPv4 address for the AP.

No static AC IPv4 address is configured by default.

IPv6 network:

```
acip ipv6 ac-ipv6-address&<1-6>
```

1.3.4 Configuring a Static IP Address for an AP Interface

Overview

On a fit AP WLAN network, an AP uses a manually configured IP address or dynamically obtains an IP address in DHCP mode. No static IP address is configured on an AP by default and an AP dynamically obtains an IP address in DHCP mode and joins an AC. If the IP address dynamically obtained by the AP is used as the static IP address, the address remains unchanged after AP restart.

Restrictions and Guidelines

- You can enable IPv6 and disable IPv4 on an AP so that the AP can join an AC based on an IPv6 address.
- When the AP has IPv6 enabled and is configured with static IPv4 and IPv6 addresses, the AP attempts to discover ACs with IPv4 and IPv6 addresses and preferentially joins the AC with an IPv4 address.
- The AP can discover ACs with IPv6 addresses through IPv6 multicast, DHCPv6, or DNSv6. When static IPv6 addresses of ACs are configured on the AP, the AP sends Discover requests to the ACs to detect the validity of the ACs and joins the optimal AC.

- After an AP interface is configured with a static IP address, DHCP is disabled by default. Before configuring a static IP address, you are advised to configure a CAPWAP control address on an AC. This prevents a failure for an AP to discover the AC on the Layer 3 network.

Configuration Steps

1. Enter the privileged EXEC mode.

```
enable
```

2. Enter the global configuration mode.

```
configure terminal
```

3. Configure a static IP address for an AP interface.

   IPv4 network:

```
apip ipv4 ipv4-address network-mask ipv4-gateway
```

   Configure a static IPv4 address for the AP.

   IPv6 network:

```
apip ipv6 enable
```

4. Enable IPv6 for the AP.

   IPv6 of an AP is disabled by default.

```
apip ipv6 address ipv6-address/prefix-length ipv6-gateway
```

   Configure a static IPv6 address for the AP.

1.3.5 Configuring a Working Mode of the AP

Overview

An AP can work in fat mode, fit mode, or cloud AP mode.

Restrictions and Guidelines

- When a wall-mounted or in-wall AP works in fat mode, the default IP address of the back-end wired interface connected to the PoE switch is 192.168.110.1/255.255.255.0, and the default IP address of the front-end wired network interface (Ethernet interface on the front of the AP) is 192.168.111.1/255.255.255.0.
- If **ap-mode fat dhcp** is configured, the AP that switches to the fat mode obtains an IP address in DHCP mode by default. In addition, if the AP that restarts has no relevant configuration, it also obtains an IP address in DHCP mode by default.
- If the wall-mounted or in-wall AP is configured with **ap-mode fat dhcp**, only the back-end wired interface obtains an IP address in DHCP mode by default, and the front-end wired network interface uses a static address by default.

- When an AP switches between any two modes of fit, fat, fat DHCP, and MACC modes, the current configuration is deleted and the AP restarts. After restart, the AP will load the default configuration for the corresponding mode.
- The default login passwords for the AP in different modes are as follows:
  - In fit mode, the default login password is **password** in user mode and **apdebug** in privileged EXEC mode.
  - In fat, fat DHCP, or MACC mode, the default login password is **admin** in user mode and there is no default login password in privileged EXEC mode.

Configuration Steps

1. Enter the privileged EXEC mode.

   ```
   enable
   ```

2. Enter the global configuration mode.

   ```
   configure terminal
   ```

3. Configure a working mode of the AP.

   ```
   ap-mode { fit | fat [ dhcp ] | macc }
   ```

   By default, an AP works in fit mode.

1.4 Monitoring

Run **show** commands to check the running status of the AP and verify the configuration effect.

Run **clear** commands to clear information.

Note

Running the **clear** command may interrupt services due to key information loss.

Run **debug** commands to check debugging information.

Note

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

Displaying

Description	Command
Displays detailed information about the CAPWAP tunnel.	**show capwap** { *index* | *ip-address* [*port*] } **detail**
Displays the status of the CAPWAP tunnel.	**show capwap state**

Description	Command
Displays CAPWAP tunnel statistics.	**show capwap** { *index* | *ip-address* [*port*] } **statistics**
Displays AP version information.	**show version** { **all** | *ap-name* }

1 Configuring iBeacon

1.1 Overview

iBeacon is a new function provided by Apple when Apple launched iOS 7 in September 2013. It is similar to the NFC technology but is different. iBeacon uses the BLE technology, specifically, it uses a broadcast frame named advertising in BLE. The advertising frame is sent regularly. Devices supporting BLE can receive the frame. iBeacon is implemented by embedding data in the format defined by a product in the payload of the advertising frame.

The iBeacon technology is implemented based on BLE and achieves the purpose of connection by connecting an iBeacon base station. It should be noted that this does not require support of the Internet. For example, if you enter a store with an iPhone or an Android phone and the store has deployed an iBeacon base station, you have entered the coverage of the iBeacon base station. In this case, the store can send information, for example, coupons or information about commodities in the store, to your phone via the base station. You can consume and get discount in the store by using the received electronic coupons.

Protocols and Standards

N/A

1.2 Features

Basic Concepts

↘ iBeacon Technology

- Beacon data consists of the following information: UUID (unique general identifier), Major, Minor, and Measured Power.
- **UUID** is a 128-bit identifier meeting the ISO/IEC11578:1996 standard.
- **Major** and **Minor**, the hexadecimal identifiers, are set by the iBeacon publisher. For example, a chain store can write regional information in **Major** and IDs of individual stores in **Minor**. In addition, when the iBeacon function is embedded in household appliances, **Major** can be used to indicate the product model and **Minor** can be used to indicate the error code to notify a fault.
- **Measured Power** is the reference received signal strength indicator (RSSI) when the iBeacon module is 1m away from the receiver.

Overview

Feature	Description
iBeacon	iBeacon packets are sent through Bluetooth broadcast.

1.2.1 iBeacon

iBeacon is implemented through transmission of Bluetooth broadcast.

Working Principle

When the iBeacon configuration is modified on a wireless controller, an iBeacon configuration packet is sent to the corresponding AP.

After the packet is received, the packet is sent in the specified format to the Bluetooth chip via I2C.After receiving the packet, the CC2541 Bluetooth chip parses the configuration packet and updates the iBeacon packet.

1.3 Configuration

Configuration	Description and Command	
Configuring iBeacon	(Optional) It is used to configure the iBeacon function.	
	ibeacon uuid major minor	Configures the iBeacon function.
Configuring iBeacon based on BT Radio	(Optional) It is used to configure iBeacon based on BT radio.	
	ibeacon uuid major minor radio	Configures the iBeacon function based on BT radio.

1.3.1 Configuring iBeacon

Configuration Effect

Configure iBeacon parameters.

Notes

If the current device does not support Bluetooth, the configuration cannot take effect.

Configuration Steps

↘ Configuring iBeacon Parameters for the Specified AP

- Optional.
- Run the **ibeacon uuid** *uuid* **major** *major* **minor** *minor* command to configure the iBeacon function in AP configuration mode.
- The iBeacon function can be configured on only AP devices supporting Bluetooth.

Command	**ibeacon uuid** *uuid* **major** *major* **minor** *minor*
Parameter	*uuid*: The value of uuid is a string consisting of 32 hexadecimal characters.

Description	*major*: The value of major is a string consisting of four hexadecimal characters. *minor*: The value of minor is a string consisting of four hexadecimal characters.
Defaults	By default, iBeacon is not configured.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the iBeacon function for an AP. For devices that do not support Bluetooth, the configuration cannot take effect.

Verification

Run the **show running** command on an AP to check whether the configuration is successful.

Configuration Examples

↘ Configuring the iBeacon Function for the Specified AP

Configuration Steps	Configure the iBeacon function for the specified AP. Directly configure iBeacon on an AP.
Configuration	Hostname(config)# ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154
Verification	After configuring the iBeacon function for the specified AP, you can check the configuration information in the following modes: On an AP device, run the **show running** command to display configuration information.
	Hostname(config)#show running ! ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154 !

1.3.2 Configuring iBeacon based on BT Radio

Configuration Effect

Configure iBeacon parameters based on BT radio.

Notes

N/A

Configuration Steps

↘ Configuring iBeacon Based on BT Radio

- Optional.

- Run the **ibeacon uuid** *uuid* **major** *major* **minor** *minor* ***radio*** *radio-id* command to configure iBeacon based on BT radio.
- The configuration takes effect on only the APs supporting Bluetooth.

Command	**ibeacon uuid** *uuid* **major** *major* **minor** *minor* **radio** *radio-id*
Parameter Description	*uuid*: The value of uuid is a string consisting of 32 hexadecimal characters. *major*: The value of major is a string consisting of four hexadecimal characters. *minor*: The value of minor is a string consisting of four hexadecimal characters. *radio-id*: The value is an integer in the range from 1 to 255. The number of supported radios varies with different products.
Defaults	By default, iBeacon is not configured.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the iBeacon function based on BT radio. The configuration takes effect on only the APs supporting Bluetooth**.**

Verification

- Run the **show running** command to on an AP to check whether the configuration is successful..

Configuration Example

↘ Configuring iBeacon Based on BT Radio

Configuration Steps	Configure the iBeacon function based on BT radio.
Configuration	Hostname# configure terminal Hostname(config)# ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154 radio 1
Verification	After configuring the iBeacon function based on BT radio, you can check the configuration information in the following modes: On an AP, run the **show running** command to display configuration information.
	Hostname# show running ! ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154 radio 1 !

1.4 Monitoring

Displaying

Description	**Command**

-	-

Configuring Wireless Security

1. Configuring RSNA
2. Configuring STA Access Control Lists
3. Configuring WIDS

1 Configuring RSNA

1.1 Overview

The Robust Security Network Architecture (RSNA) function provides security mechanisms for WLANs.

A WLAN uses open media and public electromagnetic waves as a carrier to transmit data signals. Neither communication party is connected with a cable. If transmission links are not properly protected through encryption, data transmission will be at great risk. Therefore, security mechanisms are especially important in a WLAN.

To enhance the security, a WLAN should be provided with at least the authentication and encryption mechanisms:

- Authentication mechanism: The authentication mechanism is used to authenticate users and allow only specified users (authorized users) to use network resources.
- Encryption mechanism: The encryption mechanism is used to encrypt data on wireless links to ensure that WLAN data can be received and understood only by expected users.

Protocols and Standards

- IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements -2007
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard -Aug 2004
- Information technology – Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements – 802.11, 1999 IEEE Standard for Local and metropolitan area networks "Port-Based Network Access Control" 802.1X™ -2004
- 802.11i IEEE Standard for Information technology –Telecommunications and information exchange between systems –Local and metropolitan area networks – Specific requirements

1.2 Applications

Application	Description
WEP Encryption	In a small WLAN that has a lower requirement for security; static WEP encryption can be used to protect wireless data communication.
PSK Access Authentication	For small and medium-sized enterprise networks or family users, access authentication based on pre-shared keys can be used to enhance the security of WLANs.
802.1X Access Authentication	For a scenario that has a higher requirement for security or unified management, port-based network access control can be used.

1.2.1 WEP Encryption

Scenario

In a small WLAN that has a lower requirement for security, WEP encryption can be used.

WEP encryption can use the open-system or shared-key link authentication mode. Their differences are as follows:

- When open-system link authentication is used, WEP keys can be used only for data encryption. Even if inconsistent keys are configured, users can go online; however, data transmitted after the users go online is discarded by the receiver due to key inconsistency.
- When shared-key link authentication is used, WEP keys are used for link authentication and data encryption. If inconsistent keys are configured, link authentication fails and the client cannot go online.

Deployment

- Configure WLAN on APs.
- Configure WEP encryption on APs in WLAN security configuration mode.

1.2.2 PSK Access Authentication

Scenario

Small and medium-sized enterprise networks or family users can use the WPA or WPA2 standard to enhance WLAN security. The simplest method is to use the pre-shared key authentication (referred to as WPA-PSK and WPA2-PSK respectively). In this case, WPA is similar to WEP, but users can achieve higher security through WPA and 802.11i, including more robust authentication and better encryption algorithms.

In PSK authentication, the same pre-shared key should be configured for a STA and an AP to establish connection and communication. No additional authentication server is required.

Deployment

- Configure WLAN on APs.
- Configure PSK authentication on APs in WLAN security configuration mode.
- Use this authentication with Web authentication to support Web authentication and charging.

1.2.3 802.1X Access Authentication

Scenario

In a scenario that has a higher requirement for security, 802.1X authentication can be used.

802.1X is a port-based network access control protocol. This authentication mode is used to authenticate and control STAs at the port level. STAs connected to the ports can access a WLAN if they pass the authentication; otherwise, the STAs fail to access the WLAN.

Authentication client software needs to be installed on terminals to perform 802.1X authentication. However, in some cases, some devices cannot be installed with the software, for example, wireless printers. For the sake of network management and security, although these terminals have no 802.1X authentication client software, administrators need to control the access of these terminals. MAC Authentication Bypass (MAB) provides a solution for this application.

After the MAB function is deployed for a WLAN, a wireless device can automatically probe the MAC address of a connected terminal and uses the MAC address to initiate a request to the authentication server.

Deployment

- Configure WLAN on AP1 and AP2.
- Configure authentication server on AP1 and AP2.
- Configure 802.1X authentication on AP1 and AP2 in WLAN security configuration mode.

1.3 Features

Basic Concepts

WPA

Wi-Fi Protected Access (WPA) is a wireless security draft defined by the Wi-Fi Alliance. The IEEE802.11i standard is compatible with this draft.

RSN

The IEEE802.11i standard defines the concept of Robust Security Network (RSN): and makes many improvements against various defects of the WEP encryption mechanism. The functions are equal to WPA2 launched by the Wi-Fi Alliance.

TKIP

The Temporal Key Integrity Protocol (TKIP) is an enhancement on WEP security. TKIP provides key mixing, message integrity check and key mechanism re-generation for each packet, thus eliminating hidden risks of WEP.

AES

Advanced Encryption Standard (AES) is a new encryption standard published by the National Institute of Standards and Technology (NIST) of the United States. On October 2, 2000, the Rijndael algorithm designed by Joan Daemen and Vincent Rijmen from Belgium won with its excellent performance and anti-attack capabilities, and became the new-generation encryption standard AES.

CCMP

Counter CBC-MAC Protocol (CCMP) uses AES, which is safer than TKIP.

AKM

Authentication and Key Management (AKM) is an access authentication mode for users to access a WLAN.

SAE

Simultaneous Authentication of Equals (SAE) is a peer authentication interaction. There are three encryption policies available:

- HnP: Hunting-and-Pecking loop.
- H2E: Hash to Element.
- Both: Both Hunting-and-Pecking loop and Hash-to-Element are enabled. The device determines the encryption mode according to the client capability. If both modes are supported, H2E encryption is used preferentially.

OWE

Opportunistic Wireless Encryption (OWE) does not need users to enter authentication information, and STAs and APs negotiate temporary PMKs.

Overview

Feature	Description
Link Verification	Verify the security of a wireless link before a STA associates with a WLAN.
Access Authentication	Perform authentication for a STA that accesses a WLAN.
Wireless Data Encryption	Implement security protection for communication data of a STA that accesses a WLAN.
Management Frame Encryption	Implement encryption on management frames.
WPA3 Authentication	Perform authentication for a STA that accesses a WPA3 WLAN.

1.3.1 Link Verification

Link verification refers to 802.11 authentication, which is a low-level authentication mechanism. Link verification is performed when a STA associates with an AP over 802.11, which is earlier than access authentication. Before accessing a WLAN, the STA must be authenticated over 802.11. 802.11 authentication marks the beginning of the handshake process when a STA accesses a WLAN and the first step for network connection.

The IEEE 802.11 standard defines two approaches to link authentication:

- Open-system link authentication
- Shared-key link authentication

Working Principle

Open-System Link Authentication

Open-system link authentication allows all users to access a WLAN. In this sense, no data protection is provided, which means that no authentication is performed. In other words, if the authentication mode is set to open-system authentication, all STAs that request authentication can pass the authentication.

Open-system link authentication comprises two steps:

Step 1: A STA requests authentication. The STA sends an authentication request that contains the ID (usually the MAC address) of the STA.

Step 2: An AP returns the authentication result. The AP sends an authentication response that contains information indicating whether the authentication succeeds or fails. If the authentication succeeds, the STA and AP pass the bidirectional authentication.

Figure 1-1



↘ Shared-key Link Authentication

Shared-key link authentication is another authentication mechanism in addition to the open-system link authentication. Shared-key link authentication requires that the same shared key be configured for a STA and an AP. The shared-key link authentication can be configured only in static WEP encryption whereas the open-system link authentication is available in all the other modes.

The process of shared-key link authentication is as follows:

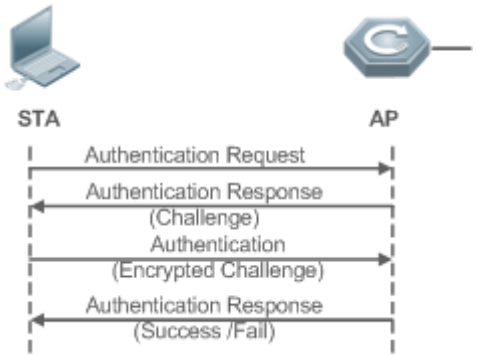
Step 1: A STA sends an authentication request to an AP.

Step 2: The AP generates a Challenge packet (a string) at random and sends the packet to the STA.

Step 3: The STA copies the received string to a new message, encrypts the message with a key and then sends the encrypted message to the AP.

Step 4: After receiving the message, the AP decrypts the message with the key, and then compares the decrypted string with the string sent to the STA. If the two strings are the same, it indicates that the STA has the same shared key as that on the AP and the shared-key authentication succeeds; otherwise, the shared-key authentication fails.

Figure 1-2



1.3.2 Access Authentication

Access authentication is a solution that enhances WLAN security.

After a STA is associated with an AP, whether the STA can use the service provided by the AP depends on the result of access authentication. If the STA passes the authentication, the AP enables the logical port for the STA; otherwise, the STA is not allowed to access the WLAN.

The IEEE 802.11 standard defines two access authentication approaches:

- PSK access authentication
- 802.1X access authentication

Working Principle

PSK Access Authentication

Pre-shared Key (PSK) is an 802.11i authentication mode, which performs authentication with pre-defined static keys. This authentication approach requires that a STA and an AP be configured with the same pre-shared key. If their keys are the same, the PSK access authentication succeeds; otherwise, the PSK access authentication fails.

802.1X Access Authentication

802.1X is a port-based network access control protocol. This authentication approach is used to authenticate and control the STAs at the port level. STAs connected to the ports can access resources in a WLAN if they pass the authentication; otherwise, the STAs cannot access resources in the WLAN.

A WLAN system with the 802.1X authentication function must provide the following elements to implement port-based authentication and authorization:

- Authentication client

Authentication client is generally installed on the STA. When the user wants to access the network, he activates the client program and enters the user name and password. Then, the client program sends a connection request.

- Authenticator

An authenticator means an AP or a communication device functioning as an AP. It is responsible for uploading and pushing user authentication information and enables or disables a port based on the authentication result.

- Authentication server

The authentication server checks whether a user has the right to use the services provided by the network system based on his identification information (user name and password), and enables or disables a port to the authentication system based on the authentication result.

MAB authentication uses a MAC address as the username to initiate a request to the authentication server. Therefore, it is not necessary for the terminal to install the client.

1.3.3 Wireless Data Encryption

Compared with a wired network, a wireless network is prone to greater security risks. Within an area, all WLAN devices share the same transmission medium and any device can receive data from all the other devices. This feature poses threat to WLAN data.

The IEEE 802.11i protocol defines the following encryption algorithms:

- WEP encryption
- TKIP encryption
- AES encryption

Working Principle

WEP Encryption

Wired Equivalent Privacy (WEP) is a data encryption mode specified in the original IEEE 802.11 standard, and is the basis for WLAN security authentication and encryption. WEP is used to promote the privacy of data exchanged between authorized users in a WLAN and prevent the data from being stolen.

WEP uses the RC4 algorithm to promote data privacy and implements authentication by using a shared key. WEP does not specify a key management scheme. Generally, keys are configured and maintained manually. WEP that does not provide a key distribution mechanism is called manual WEP or static WEP.

A WEP encrypted key may contain 64 bits or 128 bits. The 24-bit Initialization Vector (IV) is generated by the system. Therefore, a shared key to be configured on an AP and a STA consists of only 40 bits or 104 bits. In practice, the 104-bit WEP keys are widely used to replace the 40-bit WEP keys. WEP using 104-bit keys are called WEP-104. Although WEP-104 increases the security of WEP encryption, WEP encryption is prone to security risks due to limitations of the RC encryption algorithm and statically configured keys. WEP encryption cannot ensure the confidentiality and integrity of data or access authentication.

TKIP Encryption

Temporal Key Integrity Protocol (TKIP) is a temporary makeshift solution created by the IEEE 802.11 organization for fixing the WEP encryption mechanism. Like WEP encryption, TKIP encryption also uses the RC4 algorithm. But compared with WEP encryption, TKIP encryption can provide much safer protection for WLAN services in the following aspects:

A static WEP key is manually configured and all users within the same service area share the same key. A TKIP key is generated through dynamic negotiation, and each packet has a unique key.

– TKIP increases the key length from 40 bits to 128 bits, and the IV length from 24 bits to 48 bits, thus improving the security of WEP encryption.

– TKIP supports Message Integrity Check (MIC) and the replay prevention function.

AES Encryption

The Counter mode with CBC-MAC Protocol (AES-CCMP) is the most advanced wireless security protocol oriented to the public.

The IEEE 802.11i standard requires that CCMP be used to provide four security services, namely, authentication, confidentiality, integrity, and replay prevention. CCMP uses the 128-bit Advanced Encryption Standard (AES) to implement confidentiality and uses the CBC-MAC to ensure data integrity and authentication.

As a new advanced encryption standard, AES uses the symmetrical block encryption technology to provide better encryption performance than the RC4 algorithm in WEP/TKIP. It is the new-generation encryption technology that replaces WEP and brings more powerful security protection for WLANs.

1.3.4 Management Frame Encryption

Wireless management frames, such as authentication, de-authentication, association, disassociation, beacon, and probe frames, are transmitted using plaintext over the air interface. In this case, these frames may be used by illegal devices to attack wireless clients associated with APs. The Protected Management Frame (PMF) defined by the 802.11W protocol is a management frame subset, which includes frames of De-authentication, Disassociation, Spectrum Management, QoS, DLS, Block Ack, Radio measurement, SA Query, Protected Dual of Public Action, Fast BSS Transition, and Vendor-specific Protected. Packets in this subset will be encrypted when being transmitted over the air interface. The SA Query mechanism is used to prevent counterfeited association frames, de-authentication frames, and disassociation frames from disassociating STAs.

Working Principle

SA Query

When a STA is online and applies the PMF and an AP receives an association request from a counterfeited STA, the AP rejects the association request first and returns an association response with the status code 30, indicating that the association request is rejected temporarily and retry is required later. Then, the AP sends an SA Query request to the STA. If the STA is online, the STA sends an SA Query response. After the AP receives the SA Query response, it regards that the STA is online and does not process association requests within the association recovery time (10s). This prevents the real STA from being disassociated using counterfeited packets.

Similarly, when an online STA that applies the PMF receives an unencrypted disassociation or de-authentication frame, the STA sends an SA Query request to the AP. The AP returns an SA Query response. After the STA receives the SA Query response, it regards that the AP is still online and remains in the online state. This prevents the real STA from being disassociated using counterfeited packets.

1.3.5 WPA3 Authentication

Wi-Fi Protected Access 3 (WPA3) is a next-generation Wi-Fi encryption protocol released by the Wi-Fi Alliance. WPA3 is available in OWE, WPA3-Personal and WPA3-Enterprise editions. WPA3-Enterprise edition provides WPA3 Enterprise only and WPA3 Enterprise 192-bit modes.

- WPA3-Personal Edition

  WPA3-Personal uses Simultaneous Authentication of Equals (SAE) for management frame authentication to replace PSK authentication in WPA2-Personal. When a STA attempts to connect to the device enabled with WPA3-Personal, the SAE protocol used by WPA3 adds an SAE handshake before the original PSK 4-way handshake and introduces a dynamic random variable in the pairwise master key (PMK) generation process. The PMK negotiated each time is different, ensuring the randomness of the key. As such, SAE provides a more secure key authentication mechanism for WPA3 to address the security risks exposed by WPA2.

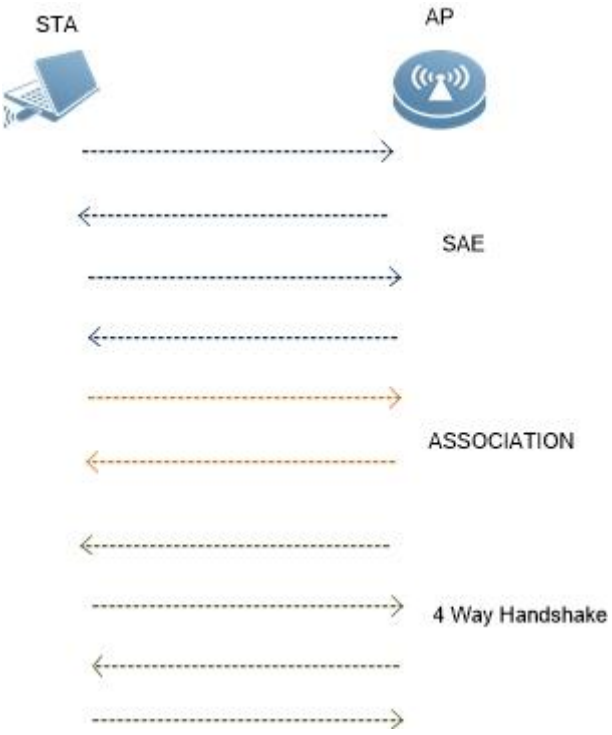
  There are three WPA3 SAE encryption options available:

  HnP: The algorithm relates the password with calculation time. It is theoretically possible to crack the password using time difference.

H2E: To address the shortcomings of HnP, the Wi-Fi Alliance introduced the Hash to Element (H2E) encryption algorithm in the third version of WPA3. In this method, the secret PWE used in the SAE protocol is generated from a password. H2E-incapable clients cannot authenticate using this encryption method.

Both: Both HnP and H2E are supported. If the client supports both encryption modes, H2E encryption is used preferentially. If not, HnP is used preferentially.

Figure 1-3 Mutual Authentication of WPA3-Personal Edition



- WPA3-Enterprise Edition

  Based on WPA2-Enterprise, the WPA3 Enterprise only mode introduces management frame protection. Deauthentication, Disassociation, Spectrum Management, QoS, DLS, Block Ack, Radio measurement, SA Query, Protected Dual of Public Action, Fast BSS, Transition, and Vendor-specific Protected packets are encrypted for transmission on the air interface to enhance security.

  Suite-B Cryptography (192 bits) suite is used for 4-way handshake in the WPA3 Enterprise 192-bit mode.

  1) Compared with the 128-bit key used by WPA2, this suite increases the key length to 192 bits, further improving the password defense strength and data security.
  2) 256-bit Galois/Counter Mode Protocol (GCMP-256) and 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) are used to protect multicast management frames.

- OWE Authentication

  Also known as enhanced open wireless authentication (Enhanced Open), it does not require users to input authentication information, but the packets exchanged between STAs and APs are still encrypted, providing a certain level of privacy and security against eavesdropping. In a scenario where OWE authentication is enabled, STAs that do not support OWE authentication are allowed to access in OPEN mode.

1.4 Configuration

Configuration	Description and Command	
Configuring Static WEP	⚠ (Mandatory) It is used to enable static WEP encryption.	
	wlansec	Enters the WLAN security configuration mode.
	security static-wep-key encryption	Enables static WEP for a WLAN and configures a static WEP key.
	⚠ (Optional) It is used to configure the link authentication mode.	
	security static-wep-key authentication	Configures the link authentication mode of static WEP.
Configuring WPA Authentication	⚠ (Mandatory) It is used to enable WPA authentication.	
	security wpa	Configures WPA authentication.
	security wpa ciphers	Configures the encryption mode of WPA authentication.
	security wpa akm	Configures the access authentication mode for WPA authentication.
	⚠ (Optional) It is used to configure a shared key for WPA PSK authentication.	
	security wpa akm psk set-key	Configures a shared key for WPA PSK authentication.
Configuring RSN Authentication	⚠ (Mandatory) It is used to enable RSN authentication.	
	security rsn	Configures RSN authentication.
	security rsn ciphers	Configures the encryption mode for RSN authentication.
	security rsn akm	Configures the access authentication mode for RSN authentication.
	⚠ (Optional) It is used to configure a shared key for RSN PSK authentication.	
	security rsn akm psk set-key	Configures a shared key for RSN PSK authentication.
Configuring MAB Authentication	⚠ (Optional) It is used to configure MAB authentication.	
	dot1x-mab	Enables MAB authentication.
Configuring Authentication Parameters	⚠ (Optional) It is used to configure key interaction parameters and the jitter prevention time in Web authentication.	
	authtimeout forbidcount	Configures the association forbidding count after four-way handshake key interaction fails.

Configuration	Description and Command	
	authtimeout forbidtime	Configures the association forbidding interval after four-way handshake key interaction fails.
	authtimeout groupcount	Configures the multicast key negotiation packet re-transmission count.
	authtimeout grouptime	Configures the timeout duration of multicast key negotiation packets.
	authtimeout paircount	Configures the uncast key negotiation packet re-transmission count.
	authtimeout pairtime	Configures the timeout duration of unicast key negotiation packets.
	webauth prevent-jitter	Configures the jitter prevention time of Web authentication.
Configuring Management Frame Encryption	⚠ (Optional) It is used to enable or disable management frame encryption.	
	security pmf { **disable** | **mandatory** | **optional** }	Enable or disable management frame encryption
Configuring WPA3 Authentication	**security wpa3 mode**	Sets the WPA3 authentication mode.
	security wpa3 personal passphrase	Sets a WPA3-Personal password.
Configures the Response Delay Mode for Authentication Packets	**rsna lazy-response enable**	Configures the response delay for authentication packets.
	rsna lazy-response time	Configures the response delay timeout for authentication packets.

1.4.1 Configuring Static WEP

Configuration Effect

- Enable static WEP encryption and provide WEP encryption protection for WLAN data.
- Configure the link authentication mode.

Notes

- The link authentication mode must be configured after static WEP encryption is enabled.
- In the security mode of a WLAN, static WEP encryption cannot be configured together with other authentication encryption.
- Only one WLAN can be configured with static WEP encryption

Configuration Steps

↘ Enabling Static WEP

- Mandatory.

- Enable static WEP encryption in WLAN security configuration mode on the AP.

Command	**security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*
Parameter Description	*key-length*: Specifies the key length, which can be 40 bits or 104 bits. **ascii**: Specifies that the WEP key is ASCII code. **hex**: Specifies that the WEP key is hexadecimal code. *key-index*: Specifies the key index, ranging from 1 to 4. *key*: Specifies key data.
Defaults	Static WEP is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to configure a static WEP key and enable static WEP. This command can be configured repeatedly, but only the last configuration takes effect. The key length must be the same as the *key-length* parameter in the command.

Configuring the Link Authentication Mode

- (Optional) The default link authentication mode is open-system link authentication. This command can be used to configure shared-key link authentication.
- The link authentication mode can be configured only after static WEP encryption is enabled. After configuring the sharedkey link authentication mode, set the link authentication mode to shared key link authentication on the STA; otherwise, the STA cannot access the WLAN.

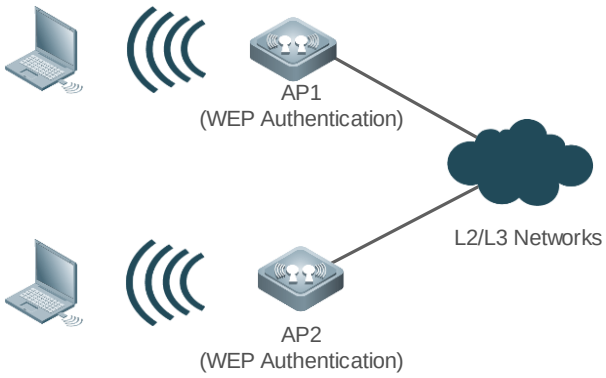
Command	**security static-wep-key authentication** { **open** | **share-key** }
Parameter Description	**open**: Configures open-system link authentication. **share-key**: Configures shared key link authentication.
Defaults	A STA accesses a WLAN by using open-system link authentication by default.
Command Mode	WLAN security configuration mode
Usage Guide	Configure the link authentication mode after configuring a static WEP key. The link authentication mode cannot be configured for other security configuration modes than static WEP.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring Static WEP Encryption and Using Shared-Key Link Authentication for WLAN 1

Scenario Figure 1-4	 In Fat AP mode, configure WLAN 1 on AP1 and AP2, and configure the security policies 1 as follows: 1. Enable static WEP encryption. 2. Configure shared-key link authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable static WEP encryption and configure a WEP key. ● Set the link authentication mode to shared-key link authentication.
AP	Hostname(config)#wlansec 1 Hostname(config-wlansec)# security static-wep-key encryption 40 ascii 1 12345 Hostname(config-wlansec)# security static-wep-key authentication share-key
Verification	Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.
AP	Hostname# show running-config | begin wlansec 1 wlansec 1 security static-wep-key encryption 40 ascii 1 12345 security static-wep-key authentication share-key !

Common Errors

- The configured key length is inconsistent with the specified key length.
- Static WEP is configured for multiple WLANs.
- The link authentication mode is configured before static WEP is enabled.

1.4.2 Configuring WPA Authentication

Configuration Effect

- Enable WPA authentication for a WLAN.
- Specify the access authentication mode and encryption mode in WPA authentication.

Notes

- When WPA authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, WPA authentication cannot be configured with WEP authentication.

Configuration Steps

Configuring WPA Authentication

- Mandatory.

Command	**security wpa** { **enable** | **disable** }
Parameter Description	**enable**: Enables WPA authentication. **disable**: Disables WPA authentication.
Defaults	WPA authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in WPA authentication only after WPA authentication is enabled; otherwise, the configuration does not take effect. When WPA authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode of WPA Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The encryption mode of WPA authentication can be configured only after WPA authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between a STA and the WLAN is protected by the corresponding encryption mode.

Command	**security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode of WPA authentication. **disable**: Disables the encryption mode of WPA authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode of WPA authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode of WPA authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. A STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security wpa akm** { **psk** | **802.1x** } { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode of WPA authentication. **disable**: Disables the access authentication mode of WPA authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for WPA Authentication

- (Optional) It must be configured when WPA PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AP.

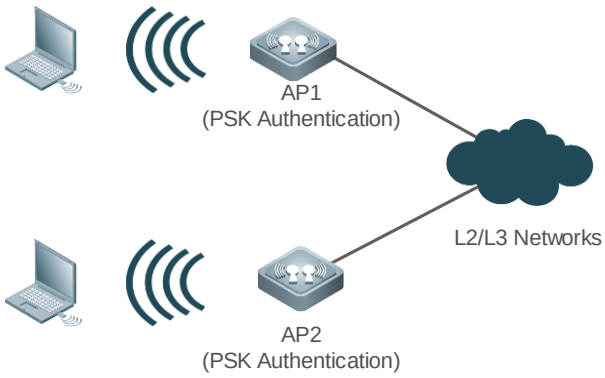
Command	**security wpa akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring WPA PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario Figure 1-5	 In Fat AP mode , configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure WPA PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable WPA authentication. ● Configure the AES encryption mode for WPA authentication. ● Configure the PSK access authentication mode for WPA authentication. ● Configure the PSK key 12345678.
AP	Hostname(config)# wlansec 1 Hostname(config-wlansec)# security wpa enable Hostname(config-wlansec)# security wpa ciphers aes enable Hostname(config-wlansec)# security wpa akm psk enable Hostname(config-wlansec)# security wpa akm psk set-key ascii 12345678
Verification	Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security wpa enable security wpa ciphers aes enable security wpa akm psk enable security wpa akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- A WPA encryption mode is configured before WPA authentication is enabled in WLAN security configuration mode.

- An access authentication mode is configured before WPA authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- A WPA PSK key is configured before WPA authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.3 Configuring RSN Authentication

Configuration Effect

- Enable RSN authentication for a WLAN.
- Specify the access authentication mode and encryption mode in RSN authentication.

Notes

- When RSN authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, RSN authentication cannot be configured with WEP authentication.

Configuration Steps

↘ Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AP.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

↘ Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.

- The encryption mode in RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between a STA and the WLAN is protected by the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode for RSN authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The access authentication mode in RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. A STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable | disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AP.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters.

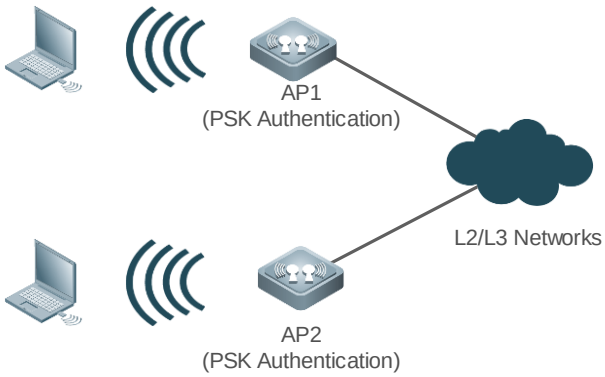
	hex: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring RSN PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario Figure 1-6	 In Fat AP mode, configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure RSN PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key to 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678.
AP	Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm psk enable Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678
Verification	Run the **show running-config**	**begin wlansec** command to check whether the configuration

	takes effect.
AP	Hostname# show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable security rsn akm psk enable security rsn akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- An RSN encryption mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- An access authentication mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- An RSN PSK key is configured before RSN authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.4 Configuring MAB Authentication

Configuration Effect

- Enable MAB authentication for a WLAN.

Notes

- In security mode of a WLAN, MAB authentication cannot be configured together with 802.1X access authentication or WEP authentication, but can be configured together with PSK authentication.

Configuration Steps

↘ Configuring MAB Authentication

- Mandatory.
- Enable MAB authentication in WLAN security configuration mode on the AP.
- Run the **dot1x-mab** command to enable MAB authentication or run the **no dot1x-mab** command to disable MAB authentication.

- MAB authentication can be configured independently, without RSN or WPA authentication enabled. MAB authentication can be used together with PSK access authentication, but cannot be used together with 802.1X access authentication.

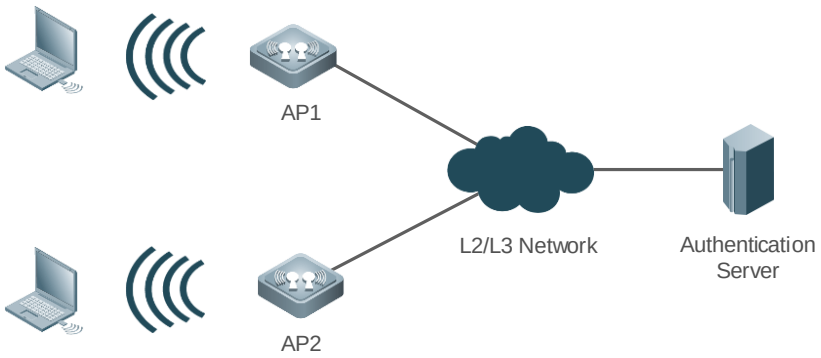
Command	dot1x-mab
Parameter Description	-
Defaults	MAB authentication is not configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable MAB authentication. MAB authentication can be used together with PSK access authentication, but cannot be used together with 802.1X access authentication.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring MAB Authentication for WLAN 1

Scenario Figure 1-7	 In Fat AP mode, configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure MAB authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable MAB authentication.
AP	Hostname# configure terminal Hostname(config)# aaa new-model Hostname(config)# radius-server host 192.168.32.120 Hostname(config)# radius-server key abcd@1234 Hostname(config)#wlansec 1 Hostname(config-wlansec)# dot1x-mab
Verification	Run the **show running-config**	**begin wlansec** command to check whether the configuration takes effect.
AP	Hostname#show running-config	begin wlansec 1 wlansec 1

	dot1x-mab !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- If 802.1X access authentication is enabled in WLAN security configuration mode, MAB authentication cannot be configured.

1.4.5 Configuring Authentication Parameters

Configuration Effect

- Configure key interaction parameters.
- Configure the jitter prevention time in Web authentication.

Notes

- Key interaction parameters take effect only in PSK or 802.1X authentication.
- The jitter prevention time in Web authentication can be configured only after Web authentication is enabled.

Configuration Steps

↘ Configuring Key Interaction Parameters

- Optional. Generally, it is unnecessary to configure key interaction parameters. It is recommended to set the packet re-transmission count and timeout duration to great values for a poor WLAN environment.
- It is configured in WLAN security configuration mode on the AP.

Command	**authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }
Parameter Description	**forbidcount** *count*: Configures the association forbidding count after four-way handshake key interaction fails. **forbidtime** *time*: Configures the association forbidding interval after four-way handshake key interaction fails. **groupcount** *count*: Configures the multicast key negotiation packet re-transmission count. **grouptime** *timeout*: Configures the timeout duration of multicast key negotiation packets. **paircount** *count*: Configures the unicast key negotiation packet re-transmission count. **pairtime** *timeout*: Configures the timeout duration of unicast key negotiation packets.
Defaults	The association is not forbidden after four-way handshake key interaction fails. The default multicast key negotiation packet re-transmission count is 4. The default timeout duration of multicast key negotiation packets is 1200 ms. The default unicast key negotiation packet re-transmission count is 4. The default timeout duration of unicast key negotiation packets is 1200 ms.

Command Mode	WLAN security configuration mode
Usage Guide	Key interaction parameters take effect only in PSK or 802.1X authentication.

Configuring the Jitter Prevention Time of Web Authentication

- Optional. The default jitter prevention time of Web authentication is 300 seconds. Users can configure the jitter prevention time based on actual requirements or disable the jitter prevention of Web authentication by setting the time to 0 seconds.
- It is configured in WLAN security configuration mode on the AP.

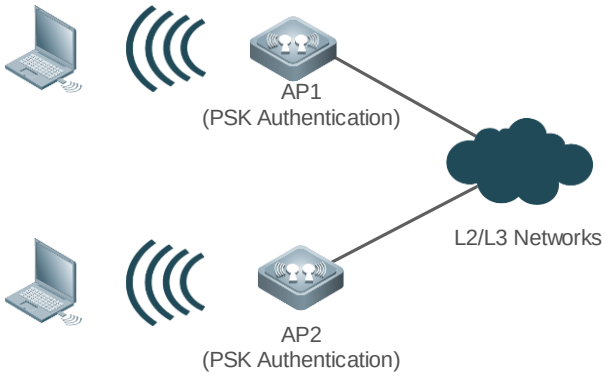
Command	**webauth prevent-jitter** *timeout*
Parameter Description	*timeout*: Configures the jitter prevention time of Web authentication, ranging from 0 to 86400 seconds (the jitter prevention of Web authentication is disabled when this parameter is set to 0).
Defaults	The default jitter prevention time of Web authentication is 300 seconds.
Command Mode	WLAN security configuration mode
Usage Guide	The jitter prevention time of Web authentication can be configured only after Web authentication is enabled.

Verification

Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.

Configuration Example

Configuring the RSN-PSK + Web Authentication Mode, the Unicast Key Negotiation Re-transmission Count to 5, and the Jitter Prevention Time of Web Authentication to 900 Seconds for WLAN 1

Scenario Figure 1-8	 In Fat AP mode, configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure RSN PSK authentication. 2. Enable Web authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678.

	● Set the unicast key negotiation packet re-transmission count to 5. ● Configure Web authentication. ● Set the jitter prevention time of Web authentication to 900 seconds.
AP	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# aaa new-model Hostname(config)# radius-server host 192.168.197.79 key webkey Hostname(config)# aaa authentication web-auth default group radius Hostname(config)# aaa accounting network default start-stop group radius Hostname(config)# web-auth template eportalv2 Hostname(config.tmplt.eportalv2)# ip 192.168.197.79 Hostname(config.tmplt.eportalv2)# url http://192.168.197.79:8080/eportal/index.jsp Hostname(config.tmplt.eportalv2)# exit Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm psk enable Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678 Hostname(config-wlansec)# authtimeout paircount 5 Hostname(config-wlansec)# webauth Hostname(config-wlansec)# webauth prevent-jitter 900
Verification	Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable security rsn akm psk enable security rsn akm psk set-key ascii 12345678 webauth prevent-jitter 900 webauth authtimeout paircount 5

Common Errors

- The jitter prevention time of Web authentication is configured before Web authentication is enabled.

1.4.6 Configuring Management Frame Encryption

Configuration Effect

- Transmit partial management frames over the air interface in ciphertext format.

Notes

- Only WPA2 supports management frame encryption. If the WLAN uses Open, WEP-40, WEP-104 or WPA (AES or TKIP) for encryption, the management frame encryption function cannot be enabled.
- Not all STAs' OSs support management frame encryption.

Configuration Steps

Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AP.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured for RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The encryption mode for RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After a data encryption mode is configured for a WLAN and a STA accesses the WLAN, communication data of the STA is protected in the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable the AES or TKIP encryption mode for RSN authentication. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The access authentication mode for RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.
  A STA can access a WLAN with access authentication enabled only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AP.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is an ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 characters. **hex**: Specifies that the PSK key is a hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	The shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Enabling Management Frame Encryption

- Mandatory.
- Enable management frame encryption on an AP.
- Management frame encryption can be configured only after RSN authentication is enabled.

Command	**security pmf** { **mandatory** | **optional** | **disable** }
Parameter Description	**mandatory**: The client needs to support management frame encryption. **optional**: The client does not need to support management frame encryption. **disable**: Disables management frame encryption.

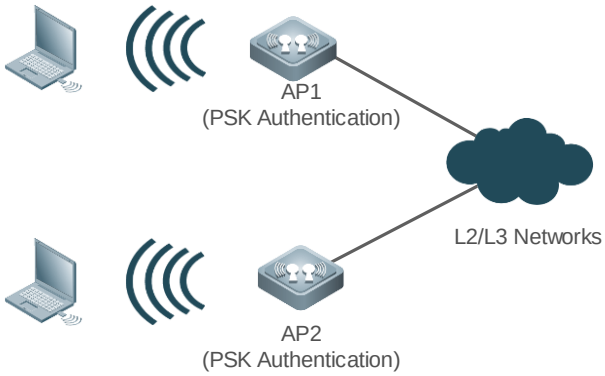
Defaults	Management frame encryption is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

Run the **show running-config | begin wlansec** command to check whether the configuration takes effect.

Configuration Example

↘ Enabling RSN-PSK Authentication and Management Frame Encryption for WLAN 1

Scenario Figure 1-9	 In Fat AP mode, configure the security policies of WLAN 1 on AP as follows: 1. Configure RSN PSK authentication. 2. Enable management frame encryption.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Set the data encryption mode for RSN authentication to AES. ● Set the access authentication mode for RSN authentication to PSK. ● Set the PSK key to 12345678. ● Enable management frame encryption.
AP	Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm psk enable Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678 Hostname(config-wlansec)# security pmf mandatory
Verification	Run the show running-config | begin wlansec command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable

	security rsn akm psk enable security rsn akm psk set-key ascii 12345678 security pmf mandatory

Common Errors

- WPA encryption is configured, but management frame encryption cannot be enabled.
- After **mandatory** is specified, a STA cannot go online because the STA does not support management frame encryption.

1.4.7 Configuring WPA3 Authentication

Configuration Effect

Enable the WPA3 authentication mode on a WLAN.

Notes

- WPA3-Personal can only work with WPA2 for authentication. WPA2 encrypts data on WLANs only using advanced encryption standard (AES).
- WPA3-Enterprise cannot be used with WPA2 simultaneously.
- WPA3 is subject to management frame encryption. Management frame encryption must be enabled before WPA3 can be enabled.
- In scenarios where WPA3-Enterprise authentication is adopted, STAs that do not support WPA3 cannot access a WLAN.

Configuration Steps

↘ Configuring Management Frame Encryption

- Mandatory.
- Perform the configuration in security configuration mode on a WLAN on the device.

Command	**security pmf** { **optional** | **mandatory** | **disable** }
Parameter Description	**mandatory**: Sets management frame encryption to mandatory mode. STAs must support management frame encryption. **optional**: Sets management frame encryption to optional mode. STAs do not need to support management frame encryption. **disable**: Disables management frame encryption.
Defaults	Management frame encryption is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	● When WPA3-Enterprise is used for authentication, management frame encryption must be set to mandatory mode. Otherwise, STAs may fail to access a WLAN. ● When WPA2 and WPA2 are used for authentication simultaneously, if management frame

	encryption is set to optional mode, STAs that support WPA2 and SAE are allowed to access a WLAN; if management frame encryption is set to mandatory mode, only WPA2 STAs that support Protected Management Frames (PMF) are allowed to access a WLAN.

Configuring the WPA3 Mode

- Mandatory.
- In WLAN security configuration mode, set the WPA3 mode.

Command	**security wpa3 mode** { **enhanced-open** | **enterprise** [**ccmp-128** | **gcmp-256**] | **none** | **personal** }
Parameter Description	**none**: Indicates that WPA3 is disabled. **enhanced-open**: Configures Opportunistic Wireless Encryption (OWE) authentication. **enterprise**： If the **ccmp-128** and **gcmp-256** parameters are not configured, GCMP-256 is used for authenticated encryption by default. **enterprise ccmp-128**: Configures CCMP-128 for WPA3-Enterprise authentication. **enterprise ccmp-256**: Configures GCMP-256 for WPA3-Enterprise authentication. **personal**: Configures WPA3-Personal authentication
Defaults	WPA3 is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	• WPA3-Personal can only work with WPA2 for authentication. WPA2 encrypts data on WLANs only using advanced encryption standard (AES). • WPA3-Enterprise cannot be used with WPA2 simultaneously. • WPA3 cannot be used with WPA simultaneously.

Configuring Equal-Cost WLANs for OWE Authentication

- (Optional) It must be used together with OWE authentication. After configuration, if the STA supports OWE authentication, it will access using OWE authentication. If the STA does not support OWE authentication, it will access in OPEN mode.

Command	**security wpa3 enhanced-open paired-wlan** { **none** | *wlan-id* }
Parameter Description	**none**: Clears the configuration of equivalent WLAN with OWE authentication. *wlan-id*: Configures the WLAN ID corresponding to the equivalent WLAN with OWE authentication.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	• The equivalent WLAN with OWE authentication must be pre-configured and set to OPEN. • QoS, Schedule, and other configurations of equivalent WLAN with OWE authentication must be consistent with those for OWE authentication. • After configuration, configure OWE authentication signals to hidden mode. An equivalent WLAN can only be associated with one OWE authentication signal.

Configuring a Password for the WPA3 Personal Mode

- The configuration is optional if WPA2 PSK authentication is enabled but mandatory when only the WPA3 Personal mode is enabled.
- STAs use the WPA2 PSK to access a WLAN in the WPA3-Personal/WPA2 mode.

Command	**security wpa3 personal passphrase** { **none** | **ascii** *word* }
Parameter Description	**none**: Clears the password. **ascii** *word*: Indicates a password in ASCII code, consisting of 8 to 63 characters.
Defaults	No password is configured for the WPA3 Personal mode by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuring WPA3 SAE Encryption Mode

- Mandatory.
- In WLAN security configuration mode, set the WPA3 SAE encryption mode.

Command	**security wpa3 personal pwe** { **hnp** | **h2e** | **both** }
Parameter Description	**hnp**: Configures HnP for WPA3 SAE authentication. **h2e**: Configures H2E for WPA3 SAE authentication. **both**: Configures both HnP and H2E for WPA3 SAE authentication. The device determines the encryption mode according to the client capability. If both modes are supported, H2E encryption is used preferentially.
Defaults	The default encryption mode is HnP.
Command Mode	WLAN security configuration mode
Usage Guide	• H2E encryption is more secure than HnP encryption. When both encryption modes are supported, H2E encryption is used preferentially. • If you configure H2E encryption, H2E-incapable clients will fail to access the network.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

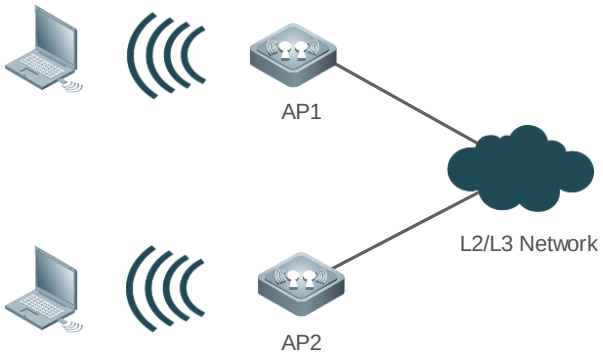
Configuration Example

Configuring the WPA3 Personal Authentication Mode for WLAN 1 with Password 12345678 and H2E Encryption Mode

Scenario	In a fat AP environment, configure the following security policies for WLAN 1: 1. Configure the pure WPA3 Personal authentication mode (RSNA disabled). 2. Set the shared key to 12345678. 3. Set the WPA3 SAE encryption mode to H2E.
Configuration	• Enter the security configuration mode of WLAN 1.

Steps	● Enable management frame encryption. ● Set the password to 12345678 for the WPA3 Personal mode. ● Set the WPA3 mode to Personal. ● Set the WPA3 SAE encryption mode to H2E.
AP	Hostname(config)#wlansec 1 Hostname(config-wlansec)#security pmf mandatory Hostname(config-wlansec)#security wpa3 personal passphrase ascii 12345678 Hostname(config-wlansec)#security wpa3 mode personal
Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security pmf mandatory security wpa3 personal passphrase ascii 12345678 security wpa3 mode personal

Configuring the WPA3-Enterprise Authentication Mode for WLAN 1

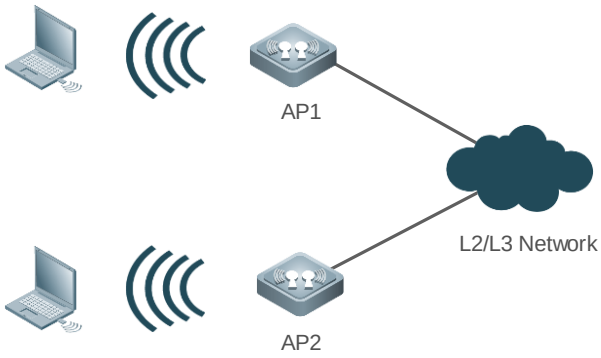
Scenario **Figure 1-10**	 In a fat AP environment, configure the following security policies for WLAN 1: 1. Configure management frame encryption. 2. Configure the WPA3-Enterprise authentication mode and set the encryption mode to the default.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Configure management frame encryption. ● Enable WPA3-Enterprise authentication mode and set the encryption mode to the default. Hostname(config)# aaa new-model Hostname(config)# aaa authentication dot1x default group radius Hostname(config)# aaa accounting network default start-stop group radius Hostname(config)# radius-server host 192.168.1.1 key daf13a124d Hostname(config)# dot1x accouting default Hostname(config)# dot1x authentication default Hostname(config)# wlansec 1 Hostname(config-wlansec)# security pmf mandatory Hostname(config-wlansec)# security wpa3 mode enterprise

Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check the configuration. Hostname#show running-config | begin wlansec 1 wlansec 1 security pmf mandatory security wpa3 mode enterprise

Configuring OWE Authentication for WLAN 1, and Configuring WLAN 2 as an Equivalent WLAN with OWE Authentication, Specifying WLAN ID as 2

Scenario

Figure 1-11



In a fat AP environment, configure the following security policies for WLAN on the AC:

1. Configure WLAN 1 to OWE authentication (ENHANCE-OPEN mode).
2. Set WLAN 2 to open.
3. Hide the SSID for WLAN 1.

Configuration Steps

- Add WLAN 1.
- Add WLAN 2.
- Enter the security configuration mode of WLAN 1.
- Enable management frame encryption.
- Configure OWE authentication. Configure WLAN 2 as an equivalent WLAN with OWE authentication.
- Enter the configuration mode of WLAN 1.
- Hide the SSID.

```
Hostname(config)#dot11 wlan 1
Hostname(config-wlan)#exit
Hostname(config)# dot11 wlan 2
Hostname(config-wlan)#exit
Hostname(config)#wlansec 1
Hostname(config-wlansec)#security pmf mandatory
Hostname(config-wlansec)#security wpa3 mode enhanced-open
Hostname(config-wlansec)#security wpa3 enhanced-open paired-wlan 2
Hostname(config-wlansec)#exit
Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)#no broadcast-ssid
Hostname(dot11-wlan-config)#exit
```

Verification	Run the **show running-config | begin wlansec** command to check whether the configuration takes effect.

AC	`Hostname#show running-config | begin wlansec 1`
	`wlansec 1`
	`security pmf mandatory`
	` security wpa3 enhanced-open paired-wlan 2`
	` security wpa3 mode enhanced-open`

Common Errors

- If you attempt to enable WPA authentication on a WLAN in WPA3 Personal mode, a configuration failure will be displayed.
- If you attempt to enable WPA2 (RSNA) authentication and set the cipher to TKIP in WPA3 Personal mode, a configuration failure will be displayed.

1.4.8 Configures the Response Delay Mode for Authentication Packets

Configuration Effect

To prevent STAs from being attacked by repeated authentication packets during the onboarding process, a response delay mode for authentication packets is added. After the response delay mode is enabled, the newly received authentication packets are discarded but previous authentication packets are still processed if association response packets are being processed within 1000 ms (by default). If the processing of association response packets has timed out (for example, association response packets are not processed properly within 1000 ms), previous association response packets are discarded and new authentication packets are processed.

Notes

N/A

Configuration Steps

↘ Configuring the Response Delay Mode

Command	**rsna lazy-response enable**
Parameter Description	This command has three forms: **rsna lazy-response enable:** Runs the command to enable the response delay mode. **no rsna lazy-response enable**: Runs the **no** form of the command to disable the response delay mode. **default rsna lazy-response enable**: Runs the **default** form of the command to restore the default configuration.
Defaults	The response delay mode is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Response Delay Timeout for Authentication Packets

Command	[**default**] **rsna lazy-response timer** *timer*
Parameter Description	*timer*: Configures the response delay timeout duration for authentication packets. The value is in milliseconds ranging from 0 to 2000. [**default**]: Restores the default configuration.
Defaults	1000
Command Mode	Global configuration mode
Usage Guide	N/A

1.5 Monitoring

Displaying

Description	Command
Displays security configuration of a WLAN.	**show wlan security** *wlan-id*
Displays security configuration of a STA.	**show wclient security** *mac-address*

1 Configuring STA Access Control Lists

1.1 Overview

STA access control lists indicate large-capacity static blacklists and whitelists and provide the following functions:

- Blacklist and whitelist for an access point (AP) or service set identifier (SSID).
- Blacklist and whitelist based on the organizationally unique identifier (OUI), matched based on the first three bytes of the vendor identifier in the media access control (MAC) address.
- The STA access control list configuration can be exported to a file or imported from a file.

Protocols and Standards

N/A

1.2 Applications

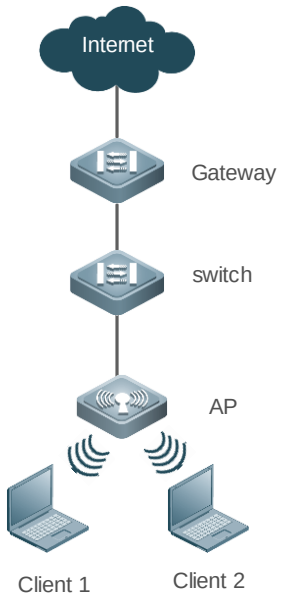
Application	Description
Fat AP Networking	Fat AP networking is adopted, including at least one AP and one STA.

1.2.1 Fat AP Networking

Scenario

On a wireless network, deploy a fat AP and enable the blacklist or whitelist of an AP or SSID, as shown in the Figure 1-1.

Figure 1-1



Remarks	PoE: switch, used as the gateway of the AP AP: wireless access point STA1 and STA2: wireless stations

Deployment

- Enable AP-based blacklist on the AP to add MAC addresses of illegal STAs to the blacklist.
- Enable SSID-based whitelist on the AP to allow STAs with specified MAC addresses to access this SSID only.

1.3 Features

Basic Concepts

N/A

Overview

Feature	Description
Configuring an AP-based Blacklist and Whitelist	Disallows STAs in the blacklist to access networks under the AP and allows STAs in the whitelist to access networks under the AP.
Configuring an SSID-based Blacklist and Whitelist	Disallows STAs in the blacklist to access the specific SSID and allows STAs in the whitelist to access the SSID.
Importing and Exporting Configurations	Exports configurations to a file or imports configurations from a file.

1.3.1 Configuring an AP-based Blacklist and Whitelist

You can add the MAC addresses of illegal STAs to the MAC address blacklist of the AP to prevent these STAs from accessing all networks under the AP.

If the network users are fixed, you can add the MAC addresses of legal STAs to the MAC address whitelist of the AP. In this case, only STAs with these MAC addresses can access networks under the AP.

To disallow or allow STAs of specific vendors to access the AP, add the OUIs of these STAs to the OUI blacklist or whitelist of the AP. In this case, STAs of these vendors are disallowed or allowed to access networks under the AP.

Working Principle

If the MAC address or OUI of an STA is in the blacklist or not in the whitelist when it goes online, the AP rejects the association request of the STA and sends an association failure response to it.

1.3.2 Configuring an SSID-based Blacklist and Whitelist

Some SSIDs may only allow specific STAs to access. In this case, you can configure an SSID-based blacklist or whitelist to prevent STAs not in the control scope to access an SSID.

To disallow or allow STAs of specific vendors to access an SSID, add the OUIs of these STAs to the OUI blacklist or whitelist of the SSID. In this case, STAs of these vendors are disallowed or allowed to access the SSID.

Working Principle

When an STA goes online through an SSID, the AP checks whether a blacklist or whitelist is configured for the SSID. If the MAC address or OUI of the STA is in the blacklist or not in the whitelist, the AP rejects the association request from the STA and sends an association failure response it.

1.3.3 Importing and Exporting Configurations

The STA access control list configuration may be large in capacity and cannot be stored together with common configuration files. You can export it to a file for backup or transfer it to another AP.

You can run an import command to import the backup configuration file to the AP to append it to the current configuration or overwrite the current configuration. Identical configurations will be merged automatically.

Working Principle

Export: Write the current configuration to the specified file in command format. The file can be exported from the AP using the **copy** command for backup or transfer.

Import: Read the specified file and import the configuration commands to the AP. In overwriting mode, configurations on the AP will be cleared in advance. In merging mode, entries in the file will be appended to the current configuration.

1.4 Configuration

Configuration	Description and Command	
Configuring an AP-based Blacklist	⚠ (Mandatory) It is used to add STAs to the AP-based blacklist.	
	blacklist mac *sta-mac*	Adds MAC addresses of STAs to the MAC address blacklist of the AP.
	blacklist vendor mac *sta-oui*	Adds OUIs of STAs to the OUI blacklist of the AP.
Configuring an AP-based Whitelist	⚠ (Mandatory) It is used to add STAs to the AP-based whitelist.	
	whitelist mac *sta-mac*	Adds MAC addresses of STAs to the MAC address whitelist of the AP.
	whitelist vendor mac *sta-oui*	Adds OUIs of STAs to the OUI whitelist of the AP.
Configuring an SSID-based Blacklist	⚠ (Mandatory) It is used to add STAs to the SSID-based blacklist.	
	blacklist mac *sta-mac* **in-ssid** *ssid-string*	Adds MAC addresses of STAs to the MAC address blacklist of an SSID.
	blacklist vendor mac *sta-oui* **in-ssid** *ssid-string*	Adds OUIs of STAs to the OUI blacklist of an SSID.
Configuring an SSID-based Whitelist	⚠ (Mandatory) It is used to add STAs to the SSID-based whitelist.	
	whitelist mac *sta-mac* **in-ssid** *ssid-string*	Adds MAC addresses of STAs to the MAC address whitelist of an SSID.
	whitelist vendor mac *sta-oui* **in-ssid** *ssid-string*	Adds OUIs of STAs to the OUI whitelist of an SSID.
Importing and Exporting Configurations	⚠ (Optional) It is used to import and export configurations.	
	export	Exports the current STA access control list configuration to a file.
	import	Imports the STA access control list configuration from a file.

1.4.1 Configuring an AP-based Blacklist

Configuration Effect

- STAs added to the MAC address blacklist cannot access all networks under the AP.
- STAs of vendors added to the OUI blacklist cannot access all networks under the AP.

Notes

- N/A

Configuration Steps

- Add MAC addresses of STAs to the MAC address blacklist of the AP.

Command	**blacklist mac** *sta-mac* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a blacklist is configured, STAs that meet the conditions are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

↘ Adding OUIs of STAs to the OUI Blacklist of the AP

Command	**blacklist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI blacklist is used to match OUIs of STAs. STAs of vendors in the OUI blacklist are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When the blacklist is enabled, an online STA that meet the conditions will be kicked offline

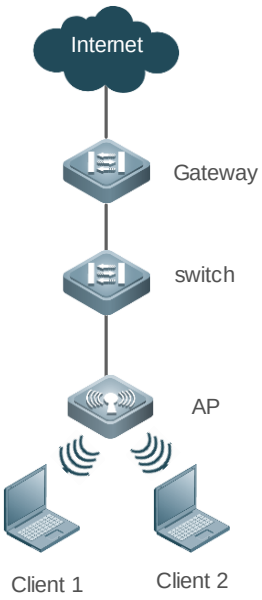
	immediately. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

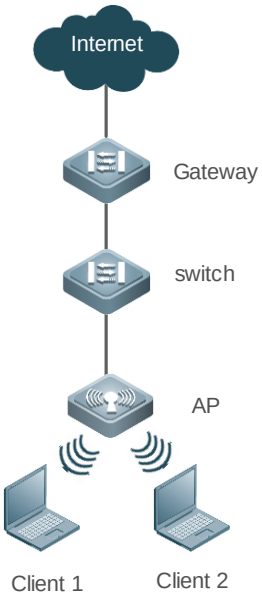
- Run the **show black-white-list blacklist** command to display the STAs in the MAC address blacklist of the AP.
- Run the **show black-white-list blacklist vendor** command to display the vendor OUIs in the OUI blacklist of the AP.

Configuration Example

↘ Configuring a MAC Address Blacklist for the AP

Scenario	
Configuration Steps	● Configure a MAC address blacklist for the AP.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist mac 0069.6c3f.2baa
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist** command. ● STAs added to the MAC address blacklist cannot associate with the AP.

Configuring an OUI Blacklist for the AP

Scenario	
Configuration Steps	● Configure an OUI blacklist for the AP.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist vendor mac 0069.6c Hostname(black-white-list)# blacklist vendor mac 0c51.01
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist vendor** command. ● STAs of vendors added to the OUI blacklist cannot associate with the AP.

Common Errors

- N/A

1.4.2 Configuring an AP-based Whitelist

Configuration Effect

- When there are entries in the MAC address whitelist, STAs not added to the whitelist cannot access any network under the AP.

- When there are entries in the OUI whitelist, STAs of vendors not added to the OUI whitelist cannot access any network under the AP.

Notes

- N/A

Configuration Steps

- Add MAC addresses of STAs to the MAC address whitelist of the AP.

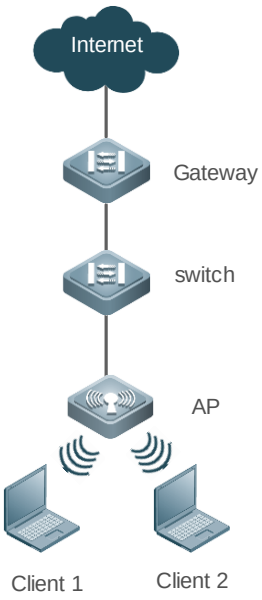
Command	**whitelist mac** *sta-mac* [**mnemonic** *string*]
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a whitelist is configured, only STAs that meet conditions are allowed to access the network. • If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When an entry is added to the whitelist, other STAs will not be kicked offline. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist** command to display the STAs in the AP-based whitelist.

Configuration Example

↘ Configuring a MAC Address Whitelist for the AP

Scenario	
Configuration Steps	● Configure a MAC address whitelist for the AP.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist mac 0069.6c3f.2baa Hostname(black-white-list)# whitelist mac 0c51.016a.5d8e
Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist** command. ● STAs not added to the whitelist cannot associate with the AP.

↘ Adding OUIs of STAs to the OUI Whitelist of the AP

Command	**whitelist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network. ● If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. ● Different types of blacklists and whitelists are complex in priority. You are advised to select a

	single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When an entry is added to the whitelist, other STAs will not be kicked offline. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Configuration Steps

↘ Adding OUIs of STAs to the OUI Whitelist of the AP

- Mandatory.

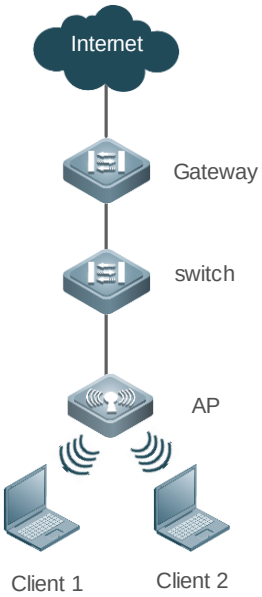
Command	**whitelist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network. ● If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. ● Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When an entry is added to the whitelist, other STAs will not be kicked offline. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist vendor** command to display the vendor OUIs in the OUI whitelist of the AP.

Configuration Example

Configuring an OUI Whitelist for the AP

Scenario	
Configuration Steps	● Configure an OUI whitelist for the AP.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist vendor mac 0069.6c Hostname(black-white-list)# whitelist vendor mac 0c51.01
Verification	● Run the **show black-white-list whitelist vendor** command to display the configuration entries. ● STAs of vendors not added to the OUI whitelist cannot associate with the AP.

Common Errors

- N/A

1.4.3 Configuring an SSID-based Blacklist

Configuration Effect

- STAs added to the MAC address blacklist of an SSID cannot access the SSID.

- When there are entries in the OUI blacklist of the specified SSID, STAs of vendors added to the OUI blacklist cannot access the SSID.

Notes

N/A

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Blacklist of the Specified SSID

Command	**blacklist mac** *sta-mac* **in-ssid** *ssid* [**mnemonic** *string*]
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a blacklist is configured, STAs that meet the conditions are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list blacklist in-ssid** *ssid* command to display the STAs in the blacklist of the SSID.

↘ Adding OUIs of STAs to the OUI Blacklist of the Specified SSID

-

Command	**blacklist vendor mac** *sta-oui* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI blacklist is used to match OUIs of STAs. STAs of vendors in the OUI blacklist are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a

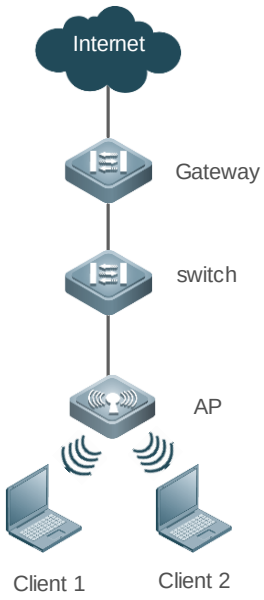
	single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list blacklist vendor in-ssid** *ssid* command to display the OUIs of vendors in the OUI blacklist of the SSID.

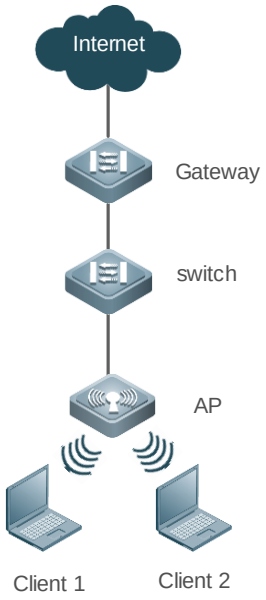
Configuration Example

↘ Configuring a MAC Address Blacklist for an SSID

Scenario	
Configuration Steps	● Configure a MAC address blacklist for SSID Hostname-web.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist mac 0069.6c3f.2baa in-ssid Hostname-web
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist in-ssid** *ssid-string* command.

	● STAs added to the blacklist cannot associate with the SSID.

Configuring an OUI Blacklist for an SSID

Scenario	
Configuration Steps	● Configure an OUI blacklist for SSID Hostname-web.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist vendor mac 0069.6c in-ssid Hostname-web Hostname(black-white-list)# blacklist vendor mac 0c51.01 in-ssid Hostname-web
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist vendor in-ssid** *ssid-string* command. ● STAs of vendors added to the blacklist cannot associate with the SSID.

Common Errors

- N/A

1.4.4 Configuring an SSID-based Whitelist

Configuration Effect

- When there are entries in the MAC address whitelist of the specified SSID, STAs not added to the MAC address whitelist cannot access the SSID.

- When there are entries in the OUI whitelist of the specified SSID, STAs of vendors not added to the OUI whitelist cannot access the SSID.

Notes

- N/A

Configuration Steps

↘ Adding MAC Addresses of STAs to the MAC Address Whitelist of the Specified SSID

Command	**whitelist mac** *sta-mac* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a whitelist is configured, only STAs that meet conditions are allowed to access the network. • If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When an entry is added to the whitelist, other STAs will not be kicked offline. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist in-ssid** *ssid* command to display the STAs in the whitelist of the SSID.

↘ Adding OUIs of STAs to the OUI Whitelist of the Specified SSID

Command	**whitelist vendor mac** *sta-oui* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network. • If the whitelist is empty, all STAs are allowed to access the network. If there is data in the

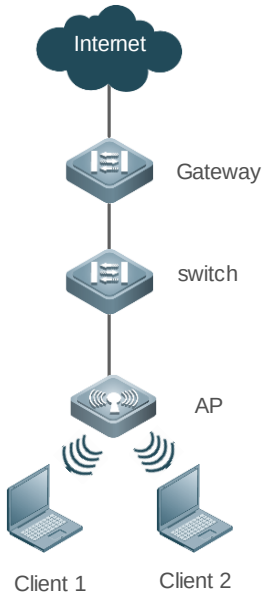
	whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. ● Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When an entry is added to the whitelist, other STAs will not be kicked offline. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist vendor in-ssid** *ssid* command to display the OUIs of vendors in the OUI whitelist of the SSID.

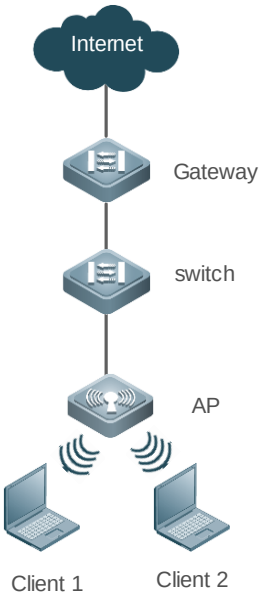
Configuration Example

↘ Configuring a MAC Address Whitelist for an SSID

Scenario	
Configuration Steps	● Configure a MAC address whitelist for SSID Hostname-web.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist mac 0069.6c3f.2baa in-ssid Hostname-web Hostname(black-white-list)# whitelist mac 0c51.016a.5d8e in-ssid Hostname-web

Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist in-ssid** *ssid-string* command. ● STAs not added to the MAC address whitelist cannot associate with the SSID.

↘ Configuring an OUI Whitelist for an SSID

Scenario	
Configuration Steps	● Configure an OUI whitelist for SSID Hostname-web.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist vendor mac 0069.6c in-ssid Hostname-web Hostname(black-white-list)# whitelist vendor mac 0c51.01 in-ssid Hostname-web
Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist vendor in-ssid** *ssid-string* command. ● STAs of vendors not added to the OUI whitelist cannot associate with the SSID.

Common Errors

- N/A

1.4.5 Importing and Exporting Configurations

Configuration Effect

- Export the current STA access control list configuration to a file.
- Import the STA access control list configuration from a file. You can select whether the imported configuration is appended to or overwrites the current configuration. If you select overwriting, clear the current configuration before importing the configuration. If you select merging, the configuration in the file will be appended to the current configuration.

Notes

- If the flash memory is insufficient during configuration export, a failure prompt is displayed.

Configuration Steps

↘ Exporting the Current Configuration to a File

- This command takes effect only once and is not saved.

Command	**export**
Parameter Description	*N/A*
Defaults	N/A
Command Mode	STA access control list configuration mode
Usage Guide	The configuration will be exported to the **black-white-list.csv** file. You can run the **copy** command to upload the file to a PC and use Excel to edit it.

↘ Importing the Configuration from a File

- This command takes effect only once and is not saved.

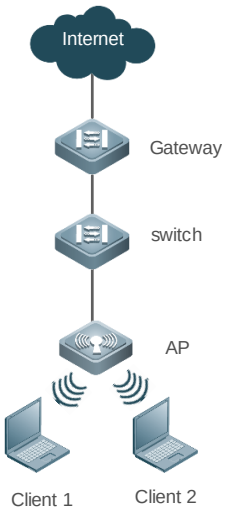
Command	**import** *filename* **{replace | append}**
Parameter Description	*N/A*
Defaults	N/A
Command Mode	STA access control list configuration mode
Usage Guide	N/A

Verification

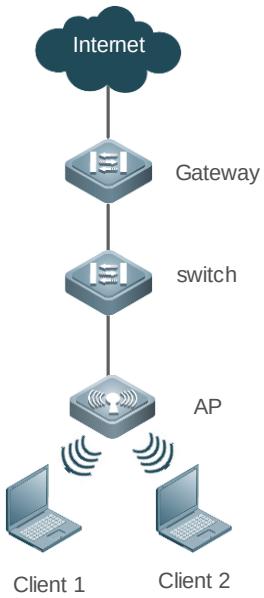
- Run the **show black-white-list config** command to display the configurations.
- Run the **dir** command to display files in the flash memory.

Configuration Example

↘ Exporting the Current Configuration to a File

Scenario	
Configuration Steps	● Export the current configuration to the **black-white-list.csv** file.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# export 10 entrys successfully exported.
Verification	● Run the **dir** command. The **black-white-list.csv** file is displayed in the output of the **dir** command. ● Run the **more black-white-list.csv** command. The file content is the STA access control list configuration.

Importing the Configuration from a File

Scenario	

Configuration Steps	● Import the configuration from the **black-white-list.csv** file and append it to the current configuration.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# import black-white-list.csv append
Verification	● Run the **show black-white-list config** command to display the configurations.

Common Errors

- N/A

1.5 Monitoring

Clearing

Description	Command
Clears entries in the MAC address blacklist of an AP or SSID.	**reset blacklist** [**in-ssid** *ssid-string*]
Clears entries in the MAC address whitelist of an AP or SSID.	**reset whitelist** [**in-ssid** *ssid-string*]
Clears entries in the OUI whitelist of an AP or SSID.	**reset whitelist vendor** [**in-ssid** *ssid-string*]
Clears entries in the OUI blacklist of an AP or SSID.	**reset blacklist vendor** [**in-ssid** *ssid-string*]

Displaying

Description	Command
Displays basic information of an STA access control list.	**show black-white-list summary**
Displays the STA access control list configuration.	**show black-white-list config**
Displays STAs in both the blacklist and whitelist.	**show black-white-list conflict**
Displays the blacklist/whitelist configuration type of a specific STA.	**show black-white-list sta-mac** *sta-mac*
Displays entries in the MAC address blacklist of an AP or SSID.	**show black-white-list blacklist** [**in-ssid** *ssid-string*]
Displays entries in the OUI blacklist of an AP or SSID.	**show black-white-list blacklist vendor** [**in-ssid** *ssid-string*]
Displays entries in the MAC address whitelist of an AP or SSID.	**show black-white-list whitelist** [**in-ssid** *ssid-string*]

Displays entries in the OUI whitelist of an AP or SSID.	**show black-white-list whitelist vendor** [**in-ssid** *ssid-string*]

Debugging

N/A

1 Configuring WIDS

1.1 Overview

Compared with wired networks, Wireless LAN (WLAN) has unparalleled advantages, such as convenient deployment, flexible use, efficient cost, and easy extension, making it more and more prevalent. However, for the openness of its channels, WLAN is much vulnerable to various network threats, such as rogue access points (APs), Ad-hoc networks, and all types of protocol attacks. Therefore, security becomes a major factor that hinders WLAN development.

Wireless Intrusion Detection System (WIDS) detects vicious STA attacks and invasions in the early stage, which helps network administrators actively observe and defend against the hidden dangers in networks in the first time.

1.2 Applications

Application	Description
Frame Filtering	Facing illegal STAs attempting to access WLAN, WIDS frame filtering helps control STA access.
User Isolation	Facing a STA intending to visit other STAs in WLAN, WIDS user isolation helps isolate their direct communication.
IDS	Facing all kinds of invasion attacks in WLAN, Intrusion Detection System (IDS) helps detect those attacks.
Rogue Detection and Containment	Illegal or rogue devices in WLAN jeopardize STAs and normal services by faking services. Facing it, Rogue detection and containment help monitor and contain them.

1.2.1 Frame Filtering

Scenario

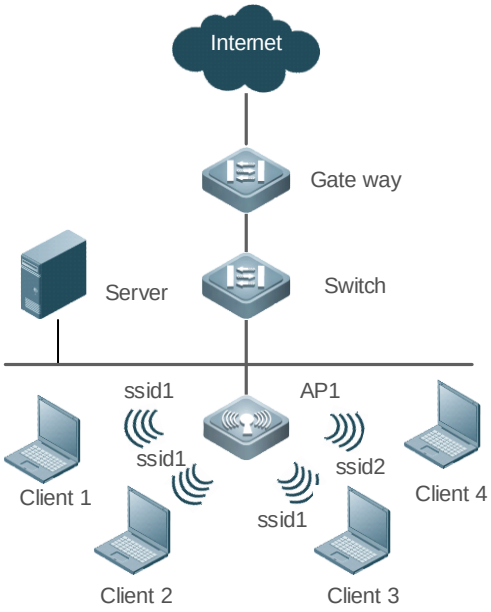
The wireless access control service is provided in WLAN, including allowing specified STAs to access WLAN or specified networks, forbidding STAs from accessing WLAN or specified networks, forbidding low-rate stations (STAs) from accessing WLAN, as well as dynamically controlling network access.

The figure below is an example, assuming that there are the following deployment requirements in the network:

- Allow Client 1 to access WLAN and Client 2 to access SSID 1.
- Prohibit Client 3 from accessing WLAN and Client 4 from accessing SSID 2.
- Filter and kick out low-rate STAs.
- Dynamically control STA access.

The networking topology is shown as follows:

Figure 1-1 Networking Topology of Wireless Access Control



Deployment

The key configuration points for the devices are:

- Add Client 1 to a WIDS whitelist. As a result, Client 1 can access the WLAN service provided by AP. Other STAs not in the list cannot.
- Add Client 2 to the SSID 1-based whitelist. As a result, Client 2 can access SSID 1 provided by AP. Other STAs not in the list cannot.
- Add Client 3 to a static blacklist. As a result, Client 3 cannot access the WLAN service provided by AP.
- Add Client 4 to the SSID 1-based blacklist. As a result, Client 4 cannot access SSID 1 provided by AP.
- Configure the low-rate threshold. STAs with rates less than the threshold will be kicked out.
- Enable the dynamic blacklist function, supporting the IDS function. After the dynamic blacklist function is enabled, any detected attack will be added into the dynamic blacklist. When the blacklist is within aging duration, the listed STAs will continue to be forbidden from communication accessed by the current AP.

1.2.2 User Isolation

Scenario

Layer 2 user isolation is provided on a WLAN, including AP-based, AP-SSID-based, AC-based, AC-SSID-based, and SSID-based user isolation.

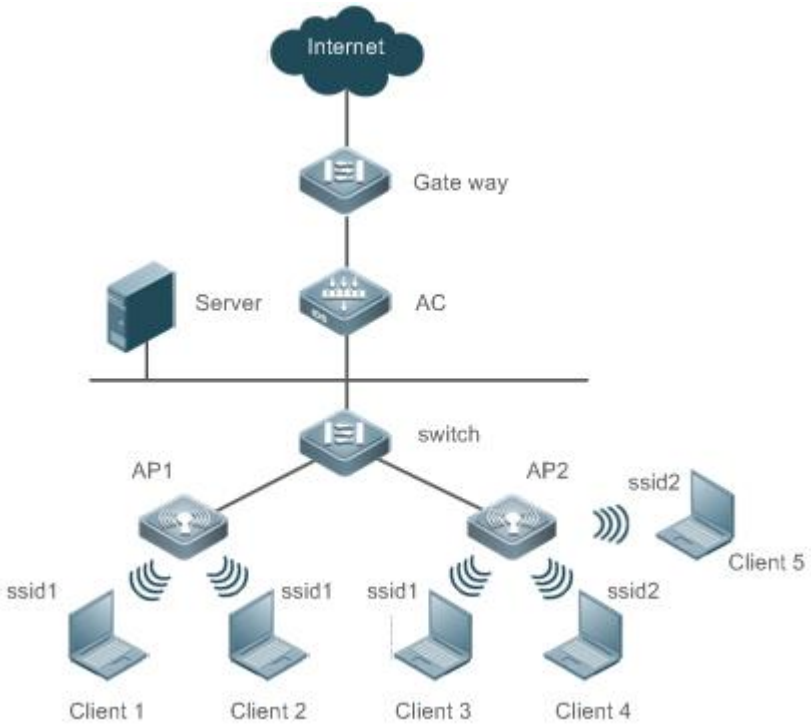
Provided that the following deployment requirements should be met on a WLAN:

1. Client 1 to Client 3 are associated with SSID 1, and Client 4 and Client 5 are associated with SSID 2. SSID 1 and SSID 2 are mapped to the same VLAN. Client 1 to Client 5 are Layer 2 users.

1. Direct communication cannot be conducted between Client 1 and Client 2, and among Client 3, Client 4 and Client 5, but can be done among other users.
2. Direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5, but can be done among other users.
3. Direct communication cannot be conducted between Client 1 and Client 3, Client 4, or Client 5, and between Client 2 and Client 3, Client 4, or Client 5, but can be done among other users.
4. Direct communication cannot be conducted between Client 3 and Client 1 or Client 2, but can be done among other users.
5. Direct communication cannot be conducted among Client 1, Client 2, and Client 3, but can be done among other users.

The networking topology is shown as follows:

Figure 1-2 Networking Topology of Wireless User Isolation



Deployment

The key configuration points for the devices are:

- Configure AP-based user isolation. As a result, direct communication can be conducted between Client 1 and Client 2, and among Client 3, Client 4, and Client 5.
- Configure AP-SSID-based user isolation. As a result, direct communication can be conducted between Client 1 and Client 2, and between Client 4 and Client 5.
- Configure AC-based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 3, Client 4, or Client 5, and between Client 2 and Client 3, Client 4, or Client 5.
- Configure AC-SSID-based user isolation. As a result, direct communication can be conducted between Client 3 and Client 1 or Client 2.

- Configure SSID1-based user isolation. As a result, direct communication cannot be conducted among Client 1, Client 2, and Client 3.

1.2.3 IDS

Scenario

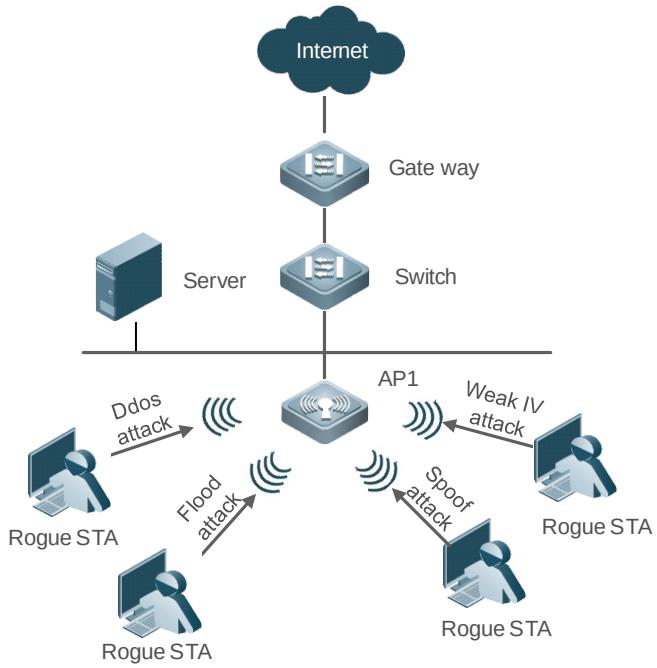
Wireless invasion attacks exist in networks, including Distributed Denial of Service (DDoS), spoofing, flooding, and Weak IV attacks. It requires APs to detect these attacks and carry out countermeasures.

Assuming there are the following deployment requirements in the network:

- DDoS attacks
- Spoofing attacks
- Flooding attacks
- Weak IV attacks

The networking topology is shown as follows:

Figure 1-3 Networking Topology of IDS



Deployment

The key configuration points for the devices are:

- Enable DDoS detection with thresholds specified which perform statistics of ARP, SYN and ICMP attack packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.

- Enable the spoofing detection with related thresholds specified to detect the deauthentication and disassociation packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable flooding detection with related thresholds specified to detect the Authentication, Association, Reassociation, Deauthentication, Disassociation, Probe, Null data and Action packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable the Weak IV detection with related thresholds specified to detect the IV value of the Web packets. If the number of continuous attacks exceeds the threshold, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.

1.2.4 Rogue Detection and Containment

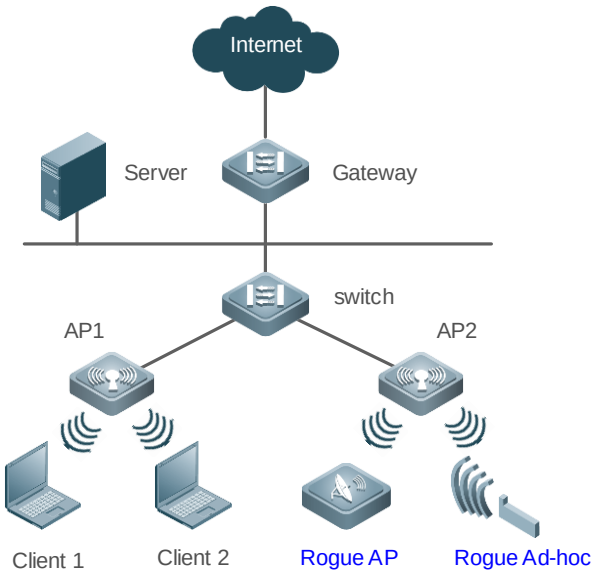
Scenario

Assuming there is the following deployment requirement in the network:

- Rogue AP and Ad-hoc devices exist in network, and detection and containment are required.

The networking topology is shown as follows:

Figure 1-4 Networking Topology of Rogue Detection and Containment



Deployment

The key configuration points for devices are:

- Enable the Monitor or Hybrid mode for a specified AP, and start the detection timer of the AP and obtain detected data at the end of each period.
- Enable the device containment and configure the mode.
- Counter the Rogue APs and Ad-hoc devices regularly based on the containment mode and detected data, preventing users from associating with fake services.

- Before the configured AP containment takes effect, confirm that WLAN is available for the AP; otherwise, the containment function will lose effect.

1.3 Features

Basic Concepts

Working Modes

The WIDS has the following working modes:

- Normal mode, providing only the access service
- Monitor mode, providing only the monitoring service
- Hybrid mode, providing both monitoring and access services

IDS Detection Types

The IDS attack detection has the following types:

- DDoS attack detection, detecting DDoS attacks involving ARP, ICMP and SYN packets
- Flooding attack detection, detecting the flooding attacks involving single-user or multi-user management packets
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication attacks
- Weak IV attack detection, detecting weak vector attacks

User Isolation Modes

The user isolation has the following modes:

- AP-based: Communication cannot proceed between layer-2 users under the same AP.
- AP-SSID based: Communication cannot proceed between layer-2 users under the same AP and in the same WLAN.
- SSID-based: Communication cannot proceed between layer-2 users in specified WLAN.

Rogue Containment Modes

The Rogue containment has the following modes:

- Ad-hoc containment mode, containing the Rogue Ad-hoc devices
- Rogue containment mode, containing the Rogue devices with over-limit RSSI
- SSID containment mode, containing illegal devices with the same SSID
- Config containment mode, containing the illegal devices in the static attack list or the SSID blacklist

Fuzzy Containment on Rogue APs

- Fuzzy match is performed based on the SSID of the rogue AP. For example, if the SSID of the local host is RUIJIE-WEB, the rogue AP whose SSID is RU1JIE-WEB can be contained after the fuzzy containment function is enabled.

- Fuzzy containment can be performed by keyword. For example, if the configured fuzzy containment keyword is ruijie, rogue APs whose SSIDs contain ruijie such as ruijie-free can be contained after the fuzzy containment function is enabled. The keyword is case-insensitive. For example, assume that the keyword is ruijie. There are 2^6 uppercase and lowercase combinations of ruijie. Once the fuzzy containment keyword is set to any of the combinations, APs whose SSIDs contain any combination of ruijie can be identified, such as RUIjie and RuiJie.

↘ Detected Devices

The types of detected rogue devices are as follows:

- APs
- Ad-hoc devices
- Unknown STAs

Overview

Feature	Description
Frame Filtering	Certain filtering rules are used to filter the packets from STAs for access control.
IDS	Timely discovers and defends against malicious or unintentional attacks in WLAN.
User Isolation	Interdicts the insecure access between STAs in WLAN to prevent disclosure of private information.
Rogue Detection and Containment	Monitors abnormal devices in the whole WLAN, helping the network administrators find hidden dangers in networks. Rogue containment refers to containing Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices in a blacklist.

1.3.1 Frame Filtering

The access control over STAs includes: low-rate filter, whitelist, static blacklist, dynamic blacklist, SSID-based whitelist and SSID-based blacklist.

Working Principle

↘ Low-Rate Filter

The low-rate filter sets a kickout threshold. When the threshold is larger than 0, the filter is enabled. If the STA rate is lower than this threshold, the STA's packets will be discarded and this STA will be disconnected.

↘ Allowlist

The whitelist includes MAC addresses of admitted STAs. If the whitelist function is enabled, only the whistlisted can access the WLAN. Other STAs will be forced to go offline and cannot access the WLAN, so as to reduce the impact of illegal packets in the WLAN.

↘ Static Blocklist

The static blacklist includes MAC address of the denied STAs. If the static blacklist function is enabled, STAs in the blacklist will be forced to go offline and cannot access the network.

Dynamic Blocklist

The dynamic blacklist includes MAC addresses of the denied STAs. You can configure the dynamic blacklist if DDoS attacks are detected. For example, add the MAC address of a detected attacker into the blacklist dynamically to forbid receiving any packet from it, thereby ensuring WLAN security.

SSID-based Allowlist

The SSID-based whitelist includes MAC addresses of the STAs admitted into a WLAN with a specified SSID. You can configure the SSID-based whitelist. If the SSID-based whitelist function is enabled, only the STAs in the whitelist of the specified WLAN are allowed to access. Other STAs cannot access the specified WLAN and online STAs that are not in the whitelist will be forced to go offline, so as to reduce the impact of illegal packets in WLAN.

SSID-based Blocklist

The SSID-based blacklist includes MAC addresses of the STAs denied by a WLAN with a specified SSID. You can configure the SSID-based blacklist. If the SSID-based blacklist function is enabled, STAs in the blacklist will be forced to go offline and cannot access this WLAN.

1.3.2 IDS

In order to timely find and defend against malicious or unintentional attacks in WLAN, IDS supports the detection on multiple attacks. When an attack is detected, an alert or a log will be generated to remind the network administrator of treatment. Based on detected results, the network administrator can timely adjust network configuration to clear the insecure factors in WLAN.

Currently, devices support the following types of IDS attack detection:

- DDoS attack detection
- Flooding attack detection
- Spoofing attack detection
- Weak IV detection

Working Principle

DDoS Attack Detection

DDoS attack means that the attackers send a large number of attack packets toward targeted devices in a short period of time (ARP packets, ICMP packets and SYN packets identified currently) so as to affect legal STAs being associated with the attacked device.

DDoS detection function performs statistics for the attacker's packets and determines whether the number of packets per second exceeds the configured threshold. If yes, this result will be logged. If the dynamic blacklist function is enabled, the attacker will be added into the dynamic blacklist.

Flooding Attack Detection

Flooding attack refers to that an attacker sends a large number of packets of the same type in a short period of time, causing the WLAN devices fail to process legal STA requests due to the Rogue flooding.

Flooding attack detection prevents this flooding attack by continuously monitoring the traffic of each device. Within specified time, when the traffic exceeds the upper limit set by the network administrator, this device is deemed to be a flooding attacker and is therefore blocked. Flooding attack detection can be used with the dynamic blacklist function. When attacks are detected, if the dynamic blacklist function is enabled, the STA initiating the attacks will be added into the dynamic blacklist, ensuring no more intrusion by this STA and thus guaranteeing network security.

↘ Spoofing Attack Detection

Spoofing attack refers to that an attacker sends fake packets in the name of another STA. For example, a fake deauthentication packet causes a STA offline.

WIDS performs detection on the broadcast deauthentication and broadcast disassociation packets. When such packet is received, it is immediately defined as a spoofing attack and logged.

↘ Weak IV Attack Detection

Weak IV (Weak Initialization Vector) attack refers to the following attack behavior: when the WLAN uses WEP encryption, an attacker intercepts packets with weak initialization vectors, cracks the shared key and finally steals the encrypted information.

When WLAN uses WEP for encryption, an initialization vector (IV) is generated for each packet and, together with the shared key, taken as input to generate a key string. With the key string and plain-text encryption, the cipher text is generated finally. When a WEP packet is sent, the IV used for packet encryption is also taken as a part of the packet header to be sent. If the IV is generated with an insecure method, for example, repetitive IVs are frequently generated or even the same IV is always generated, the shared key will be exposed easily. If a potential attacker obtains the shared key, it can control network resources and pose a threat to network security.

The IDS prevents this attack by identifying the IV of each WEP packet. When a packet with a weak IV is detected, the IDS immediately determines that this is vulnerability and logs this detected result.

1.3.3 User Isolation

Because of the mobility and uncertainty of STAs, STA information privacy appears to be particularly important in some occasions (especially public areas). Therefore, direct STA communication should be restricted. The user isolation technology can avoid insecure access between STAs in WLAN coverage (e.g., via online neighborhood), so as to prevent private information from being stolen by others.

User isolation isolates STAs, and prevents them from accessing each other without affecting their normal network access, guaranteeing service security. The layer-2 user isolation has the following types:

- AP-based user isolation
- AP-SSID based user isolation

Working Principle

↘ AP-Based User Isolation

Direct communication cannot be conducted between layer-2 STAs associated with the same AP.

AP-SSID based User Isolation

Direct communication cannot be conducted between STAs in the same WLAN who are associated with the same AP.

1.3.4 Rogue Detection and Containment

Network devices are usually divided into two types: illegal (Rogue) and legal. Rogue devices have potential vulnerabilities to be attacked or manipulated, which therefore poses a serious threat or hazard to network security. Rogue detection function can monitor abnormal devices in the whole WLAN, helping the network administrator find hidden dangers in networks.

Rogue detection is applicable to multiple Rogue devices in WLAN: APs, clients, wireless bridges, and Ad-hoc devices. Currently, only the detection on Rogue APs and Ad-hoc devices and unknown STAs is supported.

Rogue device containment counters Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices, as so to prevent STAs from accessing illegal service or illegal STAs from accessing the devices.

Working Principle

Rogue Detection

The Rogue detection function is conducted by an AP in Monitor mode or Hybrid mode. WIDS captures wireless packets in the air by deploying some APs in WLAN and setting them to operate in Monitor or Hybrid mode. By conducting analysis and statistics of monitored wireless packets, the AP can obtain information on the Rogue device. Meanwhile, the network administrator can also prepare illegal device detection rules to monitor abnormal devices in the whole WLAN.

Unknown STA Detection

The unknown STA detection function monitors the probe request packets from non-accessed STAs in the network, and the network administrator can also use configuration to specify information on the unknown STA.

Rogue Containment

The Rogue containment refers to a service which uses the means of simulating fake broadcast deauthentication packets to contain Rogue devices that meet the containment mode rules, and to prevent normal STAs from accessing Rogue devices.

Unknown STA Containment

The unknown STA containment refers to denying unknown STA access by directly constructing deauthentication packets.

1.4 Configuration

Configuration	Description and Command	
Configuring Frame Filtering	⚠ (Optional) It is used to configure frame filtering.	
	kickout threshold	Configures the low-rate kickout threshold.

Configuration	Description and Command	
	whitelist mac-address [**name** *another-name*]	Adds an entry to the whitelist.
	whitelist max	Configures the length of the whitelist.
	static-blacklist mac-address [**name** *another-name*]	Adds an entry to the static blacklist.
	static-blacklist max	Configures the length of the static blacklist.
	dynamic-blacklist enable	Enables the dynamic blacklist function.
	dynamic-blacklist lifetime	Configures the lifetime of the dynamic blacklist.
	dynamic-blacklist ap-max	Configures the length of the dynamic blacklist on APs.
	ssid-filter max	Configures the SSID-based blacklist and whitelist and their length.
	ssid-filter blacklist mac-address [**name** *another-name*]	Adds an entry to the SSID-based blacklist.
	ssid-filter blacklist max	Configures the length of the SSID-based blacklist, 256 by default.
	ssid-filter whitelist mac-address [**name** *another-name*]	Adds an entry to the SSID-based whitelist.
	ssid-filter whitelist max	Configures the length of the SSID-based whitelist, 256 by default.
Configuring IDS	⚠ (Mandatory) It is used to configure IDS.	
	attack-detection enable	Specifies the IDS type.
	attack-detection ddos	Configures the interval and packet threshold of DDoS attack detection.
	attack-detection flood multi-mac	Configures the interval and packet threshold of multi-STA flooding attack detection.
	attack-detection flood single-mac	Configures the interval and packet threshold of single-user flood attack detection.
	attack-detection spoof	Configures the interval and packet threshold of the spoofing attack detection.
	attack-detection weak-iv	Configures the interval and packet threshold of the weak IV attack detection.
	attack-detection statistics ap-max	Configures the length of IDS statistics on APs.
Configuring User Isolation	⚠ (Optional) It is used to configure user isolation.	
	user-isolation enable	Enables the AC-based, AP-based, AC-SSID-based, AP-SSID-based and CMCC layer-2 user isolation.
	user-isolation permit-mac	Adds an entry to the permissible MAC list for user isolation.

Configuration	Description and Command	
	user-isolation permit-mac max	Configures the length of the permissible MAC list for user isolation.
Configuring Rogue Detection and Containment	⚠ (Optional) It is used to set the device detection and containment function.	
	countermeasures enable	Enables the Rogue containment function.
	countermeasures ap-max	Configures the maximum number of contained devices once.
	countermeasures channel-match	Enables channel-based containment.
	countermeasures interval	Configures the containment interval.
	countermeasures mode	Configures the containment mode.
	countermeasures rssi-min	Configures the minimum containment RSSI.
	countermeasures fuzzy-enable	Enables fuzzy containment.
	countermeasures fuzzy-keyword	Configures a fuzzy containment keyword.
	device aging duration	Configures the aging duration of the detected devices.
	device attack mac-address	Adds an entry to the static attack list.
	device attack max	Configures the length of the static attack list.
	device black-ssid	Adds an entry to the SSID-based blacklist.
	device max-black-ssid	Configures the length of the SSID-based blacklist.
	device friendly-flags	Configures the device friendly flag.
	device permit mac-address	Adds an entry to the permissible MAC list.
	device permit mac-address max	Configures the length of the permissible MAC list.
	device permit ssid	Adds an entry to the permissible SSID list.
	device permit max-ssid	Configures the length of the permissible SSID list.
	device permit vendor bssid	Adds an entry to the permissible vendor list.
	device permit vendor bssid max	Configures the length of the permissible vendor list.
	device unknown-sta dynamic-enable	Enables unknown STA detection and containment.
	device unknown-sta mac-address	Adds an entry to the unknown STA list
	device unknown-sta mac-address max	Configures the length of the unknown STA list.
	device unknown-sta report enable	Enables unknown STA detection information reporting.
	device channel-bind radio	Configures the scanning channel of a specified radio.
	device detected-ap-max	Configures the maximum number of detected APs.

Configuration	Description and Command	
	hybrid-scan radio	Configures the scanning status of a specified radio.
	scan-channels { 802.11a | 802.11b | 6GHz} channels	Configures the scanning channel of a specified AP.
	scan-channels { dual-band | all-band }	Configures automatic dual-radio switchover and scanning.
Configuring AP Working Mode	⚠ (Optional) It is used to set the AP working mode.	
	device mode	Configures the AP working mode.

1.4.1 Configuring Frame Filtering

Configuration Effect

- Configure the frame filtering rules to provide packet filtering services.

Notes

- A STA cannot be configured in both the static blacklist and the whitelist.
- A STA cannot exist in both the blacklist and whitelist of the same SSID.

Configuration Steps

↘ Configuring the Low-Rate Filter

- (Optional) The **kickout threshold** command is used in WIDS configuration mode to configure the low-rate kickout threshold. The low-rate filtering function effectively works only after the low-rate kickout threshold is configured (larger than 0).
- Unless otherwise noted, enable this function only on devices which needs to support the low-rate STA filtering function.

Command	**kickout threshold** *rate*
Parameter Description	*rate*: Indicates the low-rate kickout threshold ranging from 0 to 130 Mbps.
Defaults	By default, low-rate STAs are not filtered out, and the kickout threshold is 0.
Command Mode	WIDS configuration mode
Usage Guide	The STAs can select different low-rate STA filtering thresholds based on requirements.

↘ Configuring the STA Disconnection Function

- (Optional) The **kickout client** command is used in WIDS configuration mode to disconnect online STAs.

Command	**kickout client** *H.H.H*
Parameter Description	*H.H.H*: Indicates the MAC address of a STA that is disconnected.

Defaults	N/A
Command Mode	WIDS configuration mode
Usage Guide	This command can be used to disconnect a specified online STA.

Configuring the Allowlist

- Optional.
- Run the **whitelist mac-address** command to add an entry to the whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **whitelist max** command to configure the maximum number of entries in the whitelist in WIDS configuration mode.
- If the address whitelist is configured, all online STAs whose addresses are not in the whitelist will be forced to go offline 1 minute after the last configuration command is executed.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**whitelist** { **mac-address** *H.H.H* [**name** *another-name*] | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a whitelist entry. **name** *another-name*: Indicates the another-name of the MAC address in the whitelist. **max** *num*: Indicates the length of the whitelist ranging from 1 to 2,048.
Defaults	By default, the whitelist is empty and the whitelist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The whitelist function takes effect only when the whitelist has entries.

Configuring the Static Blocklist

- Optional.
- Run the **static-blacklist mac-address** command to add an entry to the static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **static-blacklist max** command to configure the maximum number of entries in the static list in WIDS configuration mode, indicating the maximum number of permissible static blacklist entries on the device.
- After the MAC address of a STA is added to the static blacklist, the STA will be forced to go offline immediately if the STA is online.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**static-blacklist** { **mac-address** *H.H.H* [**name** *another-name*] | **max** *num* }

Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static blacklist entry. **name** *another-name*: Indicates the another-name of the MAC address in the static blacklist. **max** *num*: Indicates the length of the static blacklist ranging from 1 to 2,048.
Defaults	By default, the static blacklist is empty and the static blacklist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The static blacklist function takes effect only when the static blacklist has entries.

Configuring the Dynamic Blocklist

- Optional.
- Run the **dynamic-blacklist enable** command to enable the dynamic blacklist function in WIDS configuration mode. A dynamic blacklist entry is generated dynamically along with the IDS attack detection and works only after the dynamic blacklist function is enabled.
- Run the **dynamic-blacklist lifetime** command to configure the service life of the dynamic blacklist in WIDS configuration mode, indicating how long the dynamic blacklist exists in the device.
- Run the **dynamic-blacklist ap-max** command to configure the maximum number of dynamic blacklist entries on APs in WIDS configuration mode.
- Run the **dynamic-blacklist mac-adress** command to configure the dynamic blocklist in WIDS configuration mode.

Command	**dynamic-blacklist** { **enable** | **lifetime** *time* | **ap-max** *num* }
Parameter Description	**enable**: Enables the dynamic blacklist function **lifetime** *time*: Indicates the service life of the dynamic blacklist ranging from 60 to 86,400 seconds. **ap-max** *num*: Indicates the length of the dynamic blacklist on APs.
Defaults	By default, the dynamic blacklist function is disabled. The default length of the dynamic blacklist is 4,096 with 300-second lifetime.
Command Mode	WIDS configuration mode
Usage Guide	A dynamic blacklist entry is generated in the IDS attack detection function.

Configuring the SSID-Based Blocklist

- Optional.
- Run the **ssid-filter blacklist mac-address** command to add an entry to the SSID-based static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **ssid-filter blacklist max** command to configure the maximum number of entries in the SSID-based static blacklist in WIDS configuration mode.
- After the MAC address of a STA is added to the blacklist, the STA will be forced to go offline immediately if the STA is online and associated with the SSID.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.

- The another-name is null if it is not configured.

Command	**ssid-filter** { **max** *num* | **blacklist mac-address** *H.H.H* [**name** *another-name*] **in-ssid** *string* | **blacklist max** *num* }
Parameter Description	**max** *num*: Indicates the maximum length of the SSID-based blacklist, ranging from 1 to 128. The default is 64. **blacklist mac-address** *H.H.H* **in-ssid** *string*: Adds an entry to the specified SSID-based blacklist. **name** *another-name*: Indicates the another-name of the MAC address in the specified SSID blacklist. **blacklist max** *num*: Configures the length of the SSID-based blacklist, ranging from 1 to 2048.
Defaults	The SSID-based blacklist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based blacklist has entries. The maximum number of the SSID blacklist is 32768. To change the value of **ssid-filter blacklist max**, please ensure the product of **ssid-filter max** and **ssid-filter blacklist max** is smaller than 32768. For example, if the value of **ssid-filter blacklist max** is 2048, then the value of **ssid-filter max** can not exceed 16.

Configuring the SSID-Based Allowlist

- Optional.
- To configure the SSID-based whitelist entry, the same as above.
- To configure the SSID-based whitelist length, the same as above.
- Run the **ssid-filter whitelist mac-address** command to add an entry to the SSID-based whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **ssid-filter whitelist max** command to configure the maximum number of entries in the SSID-based whitelist in WIDS configuration mode.
- After the SSID-based whitelist is configured, STAs that are not in the whitelist of this SSID will be forced to go offline.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**ssid-filter** { **whitelist mac-address** *H.H.H* [**name** *another-name*] **in-ssid** *string* | **whitelist max** *num* }
Parameter Description	**whitelist mac-address** *H.H.H* **in-ssid** *string*: Configures the whitelist entry for a specified SSID. **name** *another-name*: Indicates the another-name of the MAC address in the specified SSID whitelist. **whitelist max** *num*: Configures the length of the SSID-based whitelist, ranging from 1 to 2048.
Defaults	The SSID-based whitelist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based whitelist has entries.

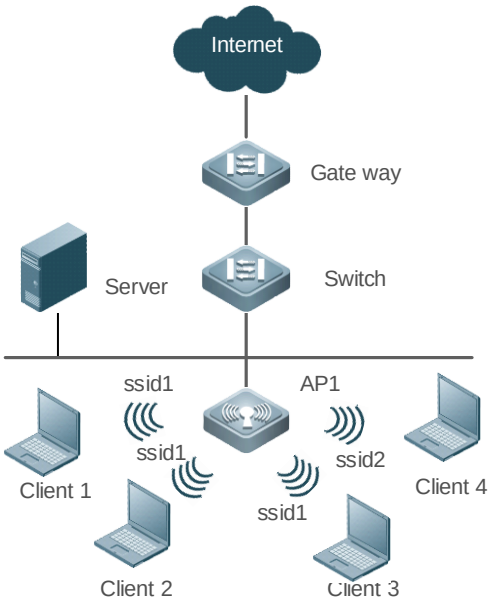
Verification

Conduct related function verifications based on corresponding frame filtering rules.

- Check the low-rate STA filtering function. The packets are discarded and the low-rate STAs are successfully removed.
- Check the whitelist function. When the whitelist is configured, the STAs not included in the whitelist cannot join the AP.
- Check the static blacklist function. When the static blacklist is configured, the STAs included in the static blacklist cannot join the AP.
- Check the dynamic blacklist function. When the dynamic blacklist function is enabled, entries in the dynamic blacklist can be generated along with the IDS attack detection, and STAs in the dynamic blacklist cannot join the AP again.
- Check the SSID-based blacklist function. When the SSID-based blacklist is configured, STAs in the SSID-based blacklist cannot join this SSID service.
- Check the SSID-based whitelist function. When the SSID-based whitelist is configured, STAs not included in the SSID-based whitelist cannot join this SSID service.

Configuration Example

↘ Configuring the Allowlist Entry

Scenario **Figure 1-5**	
Configuration Steps	● Add an entry to the whitelist on AP.
	Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# whitelist mac-address 0000.0000.0001
Verification	After the STA configures the whitelist entry, the following methods can be used to check the

	configuration. ● Run the **show wids whitelist** command to display the information on related parameters configured on the STA. ● Use the device to verify whether the function has taken effect.
	Hostname# show wids whitelist ---------- White list Information ---------- Total num:1 NUM MAC-ADDRESS NAME 1 0000.0000.0001

Common Errors

N/A

1.4.2 Configuring IDS

Configuration Effect

- IDS can be used to timely find and defend against malicious or unintentional attacks in WLAN.

Notes

- IDS needs to be used together with the dynamic blacklist function, to effectively prevent attacks against WLAN.

Configuration Steps

↘ Specifying the IDS Type

- (Optional) IDS is disabled by default.
- To configure the IDS attack detection, the same as above.

Command	**attack-detection enable** { **all** | **ddos** | **flood** | **spoof** | **weak-iv** }
Parameter Description	**ddos**: Enables DDoS attack detection. **flood**: Enables flooding attack detection. **spoof**: Enables spoofing attack detection. **weak-iv**: Enables Weak IV attack detection. **all**: Enables all IDS attack detection.
Defaults	All IDS attack detection is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

↘ Configuring DDoS Attack Detection

- Optional.

- To configure the thresholds and intervals of a specified type of packets in DDoS attack detection, the same as above.

Command	**attack-detection ddos** { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }
Parameter Description	**arp-threshold** *num*: Indicates ARP packet threshold ranging from1 to 10,000 pps. **icmp-threshold** *num*: Indicates ICMP packet threshold ranging from110,000 pps. **syn-threshold** *num*: Indicates SYN packet threshold ranging from1 to 10,000 pps. **interval** *time*: Indicates the period of DDoS attack detection ranging from 10 to 60 seconds.
Defaults	By default, the interval of DDoS attack detection is 30 seconds, and the three DDoS attack detection thresholds are 50 pps for ARP packets, 100 pps for ICMP packets, and 50 pps for SYN packets.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Flooding Attack Detection

- (Optional) Flooding attack detection is disabled by default.
- To configure the threshold and interval of a specified types of packets in flooding attack detection, the same as above.
- Run the **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time* command to configure the threshold and interval of a specified type of packets for single-STA flooding attack in WIDS configuration mode.
- Run the **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time* command to configure the threshold and interval of a specified type of packets for multi-STA flooding attack in WIDS configuration mode.

Command	**attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** } **threshold** *threshold-num* **interval** *interval-time*
Parameter Description	**single-mac**: Indicates single STA detection. **total**: Indicates all packets. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *threshold-num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 5,000. *interval-time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 4,800 for multi-STA, and 10 seconds of the statistic interval
Command	WIDS configuration mode

Mode	
Usage Guide	N/A

Command	**attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time*
Parameter Description	**multi-mac**: Indicates multi-STA detection. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *threshold-num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 10,000. *interval-time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 4,800 for multi-STA, and 10 seconds of the statistic interval
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Spoofing Attack Detection

- (Optional) Spoofing attack detection is disabled by default.
- To configure the threshold and interval of a specified type of packets in spoofing attack detection, the same as above.

Command	**attack-detection spoof** { **threshold** *threshold-num* | **interval** *interval-time*}
Parameter Description	*threshold-num*: Indicates the packet threshold of spoofing attack detection ranging from 1 to 1,000. *interval-time*: Indicates the interval of spoofing attack detection ranging from 1 to 60 seconds.
Defaults	By default, the packet threshold is 1 and the detection interval is 50 seconds.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Weak IV Attack Detection

- (Optional) The Weak IV attack detection function is disabled by default.
- To configure the thresholds and intervals for specified types of packets in Weak IV attack detection, the same as above.

Command	**attack-detection weak-iv** { **threshold** *num* | **interval** *time* }
Parameter	**threshold** *num*: Indicates the packet threshold of weak IV attack detection ranging from 1 to

Description	10,000. **interval** *time*: Indicates the interval of weak IV attack detection ranging from 1 to 60 seconds.
Defaults	The default interval of Weak IV detection is 15 seconds, and the default detection threshold is 10.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Length of IDS Statistics on APs

- Optional.

Command	**attack-detection statistics ap-max** *num*
Parameter Description	*num*: Indicates the number of APs on which IDS statistics is performed. The value ranges from 1 to 1024.
Defaults	The default value is 512.
Command Mode	WIDS configuration mode
Usage Guide	N/A

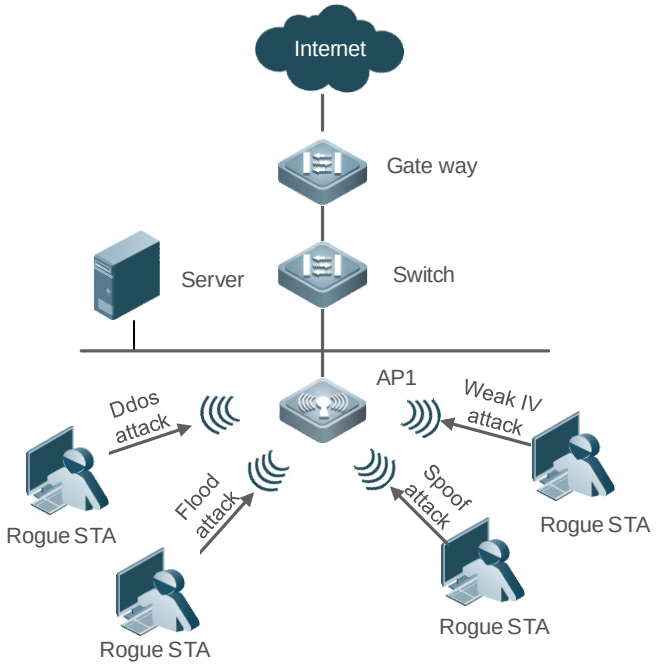
Verification

Carry out related verifications based on the IDS attack detection type:

- DDoS attack detection, detecting the ARP packet attack, ICMP packet attack and SYN packet attack.
- Flooding attack detection, detecting the multi-STA flooding attack and single-STA flooding attack.
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication packet attacks.
- Weak IV attack detection, detecting the weak IV packet attack.

Configuration Example

Configuring DDoS Attack Detection

Scenario **Figure 1-6**	
Configuration Steps	● Specify the IDS type and configure related thresholds on AP. Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# attack-detection enable flood Hostname(config-wids)# attack-detection ddos interval 10
Verification	● If a DDoS attack exists, related syslog information will be printed on AP. *Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ARP DDOS attack to Ap (1414.0902.0016). Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ICMP DDOS attack to Ap (1414.0902.0016). Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): SYN DDOS attack to Ap (1414.0902.0016).

Common Errors

N/A

1.4.3 Configuring User Isolation

Configuration Effect

- After user isolation is configured, direct communication cannot be conducted between STAs meeting the user isolation rules.

Notes

- User isolation is only valid for layer-2STAs.

Configuration Steps

Configuring the User Isolation Mode

- Optional.
- Unless otherwise noted, configure this function on ACs.

Command	**user-isolation** { **ap** | **ssid-ap** } **enable**
Parameter Description	**ap:** Indicates AP-based layer-2 user isolation. **ssid-ap:** Indicates AP-SSID-based layer-2 user isolation.
Defaults	User isolation is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Permissible MAC List for User Isolation

- Optional.
- Unless otherwise noted, configure this information on devices.
- To configure the isolation list length, the same as above.

Command	**user-isolation permit-mac** { *H.H.H* | **max** *num* }
Parameter Description	*H.H.H*: Indicates the permissible MAC list entry for user isolation. **max** *num*: Indicates the permissible MAC list length for user isolation ranging from 1 to 2,048.
Defaults	The permissible STA's MAC list for isolation is empty, with the default length of 1,024.
Command Mode	WIDS configuration mode
Usage Guide	N/A

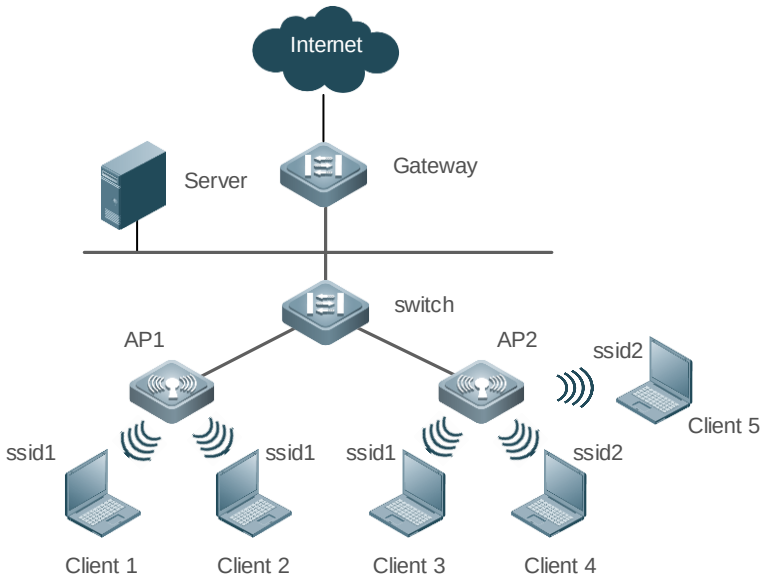
Verification

- Carry out related verifications based on the isolation mode.

Configuration Example

Configuring User Isolation

Scenario	

Figure 1-7	
Configuration Steps	● Configure the AP-based layer-2 user isolation on the AP.
	Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# user-isolation ap enable
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA.
	Hostname#show running-config ... ! wids user-isolation ap enable !

Common Errors

N/A

1.4.4 Configuring Rogue Detection and Containment

Configuration Effect

Configure Rogue detection and containment provide illegal device suppression and maintain WLAN security.

Notes

The detection and containment of Rogue devices takes effect only when the AP working mode is Hybrid or Monitor.

Configuration Steps

Enabling Rogue Containment

- Optional. Run the **countermeasures enable** command to enable Rogue containment in WIDS configuration mode.

Command	**countermeasures enable**
Parameter Description	N/A
Defaults	Rogue containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Interval

- Optional. Run the **countermeasures interval** *time* command to configure the interval of Rogue containment in WIDS configuration mode.

Command	**countermeasures interval** *time*
Parameter Description	*time*: Indicates the containment interval ranging from 100 to 10,000 ms.
Defaults	The default containment interval is 1,000 ms.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Mode

- Optional.
- Run the **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** } command to configure the Rogue containment mode in WIDS configuration mode.

Command	**countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }
Parameter Description	**adhoc**: Indicates Ad-hoc containment mode, countering Ad-hoc devices. **config**: Indicates Config containment mode, countering devices which meet entries in the SSID blacklist and static attack list. **rogue**: Indicates Rogue containment mode, countering devices whose RSSI is larger than the threshold. **ssid**: Indicates SSID containment mode, countering devices with the same SSID but not on the same device. **all**: Indicates all the above containment modes.
Defaults	No containment mode is specified by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the device operates in Normal mode.

Configuring the Static Attack List

- Optional. Run the **device attack mac-address** *H.H.H* command to configure the static attack statistic list information in WIDS configuration mode.

Command	**device attack** { **mac-address** *H.H.H* | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static attack list entry. **max** *num*: Indicates the length of the static attack list, ranging from 1 to 1,024.
Defaults	The static attack list is empty, and the length of the static attack list is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the SSID-based Blocklist

- Optional. Run the **device black-ssid** *ssid* command to configure the SSID blacklist information in WIDS configuration mode.

Command	**device** { **black-ssid** *ssid* | **max-black-ssid** *num* }
Parameter Description	**black-ssid** ssid: Indicates the SSID blacklist entry. **max-black-ssid** *num*: Indicates the SSID blacklist length, ranging from 1 to 1,024.
Defaults	The SSID blacklist is empty, and the SSID blacklist length is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Lists of Permissible MACs, SSIDs and Vendors

- Optional.
- Run the **device permit mac-address** *H.H.H* command to configure the permissible MAC list entry in WIDS configuration mode.
- Run the **device permit ssid** *H.H.H* command to configure the permissible SSID list entry in WIDS configuration mode.
- Run the **device permit vendor** *H.H.H* command to configure the permissible vendor list entry in WIDS configuration mode.

Command	**device permit** { **mac-address** *H.H.H* | **mac-address max** *num* | **ssid** *ssid* | **max-ssid** *num* | **vendor bssid** *H.H.H* | **vendor bssid max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the permissible MAC list entry, null by default. **mac-address max** *num*: Indicates the permissible MAC list length, ranging from 1 to 2,048, 1,024 by default. **ssid** *ssid*: Indicates the permissible SSID list entry, null by default. **max-ssid** *num*: Indicates the permissible SSID list length, ranging from 1 to 1,024, 512 by default. **vendor bssid** *H.H.H*: Indicates the permissible vendor list entry, null by default. **vendor bssid max** *num*: Indicates the permissible vendor list length, ranging from 1 to 1,024, 512 by default.
Defaults	N/A
Command Mode	WIDS configuration mode

Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Maximum Number of Contained Devices Once

- Optional.
- Run the **countermeasures ap-max** *ap-num* command to configure the quantity of one-time Rogue device containment in WIDS configuration mode.
- Unless otherwise noted, configure this on devices which need to configure the contained Rogue device quantity.

Command	**countermeasures ap-max** *ap-num*
Parameter Description	*ap-num*: Indicates the maximum number of countered devices each time, ranging from 1 to 256.
Defaults	The default maximum number of countered devices is 30.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Aging Duration of the Detected Devices

- Optional. Run the **device aging duration** *time* command to configure the aging duration of the detected devices in WIDS configuration mode.

Command	**device aging duration** *time*
Parameter Description	*time*: Indicates the aging duration, ranging from 500 to 5,000 seconds.
Defaults	The default aging duration is 1,200 seconds.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Device Friendly Flag

- Optional.
- Run the **device friendly-flags** *value* command to configure the device friendly flag in WIDS configuration mode. With the device friendly flag, the device can identify devices on the same device.

Command	**device friendly-flags** *value*
Parameter Description	*value*: Indicates the device friendly flag, ranging from 1 to 4294967295.
Defaults	The default value is 0.
Command Mode	WIDS configuration mode
Usage Guide	By configuring the friendly flag, AP is able to recognize a friendly AP. The default is random configuration.

Configuring the Minimum Containment RSSI

- Optional.

- Run the **countermeasures rssi-min** *num* command to configure the minimum containment RSSI in WIDS configuration mode. A Rogue device which exceeds this RSSI will be countered.

Command	**countermeasures rssi-min** *num*
Parameter Description	*num*: Indicates the minimum containment RSSI, ranging from 0 to 75 (-95 to -20).
Defaults	The default minimum containment RSSI is 25 (-70) by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Enabling Channel-Based Containment

- Optional. Run the **countermeasures channel-match** command to enable channel-based containment function in WIDS configuration mode. The channel-based containment can be conducted based on the channel on which the detected Rough device operates.

Command	**countermeasures channel-match**
Parameter Description	**N/A**
Defaults	Channel-based containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring Fuzzy Containment

- Optional.
- Run the **countermeasures fuzzy-enable** command to configure the fuzzy containment function in WIDS configuration mode. Fuzzy match is performed based on the SSID of the rogue AP. For example, if the SSID of the local host is RUIJIE-WEB, the rogue AP whose SSID is RU1JIE-WEB can be contained after the fuzzy containment function is enabled.
- Unless otherwise specified, configure the fuzzy containment function on devices which require this function.

Command	**countermeasures fuzzy-enable**
Parameter Description	N/A
Defaults	The fuzzy containment function is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	If containment modes include the configuration containment mode, rogue APs whose SSID are similar to those in the SSID blacklist are contained. If containment modes include the SSID containment mode, rogue APs whose SSIDs are similar to the SSID of the local host are contained. Fuzzy containment takes effect only in configuration containment mode and SSID containment mode.

Configuring a Fuzzy Containment Keyword

- Optional. Run the **countermeasures fuzzy-keyword** *string* command to configure a fuzzy containment keyword in WIDS configuration mode. Fuzzy containment can be performed by keyword. For example, if the configured fuzzy containment keyword is ruijie, rogue APs whose SSIDs contain ruijie such as ruijie-free can be contained after the fuzzy containment function is enabled. The keyword is case-insensitive. For example, assume that the configured fuzzy containment keyword is ruijie. There are 2^6 uppercase and lowercase combinations of ruijie. Once the fuzzy containment keyword is set to any of the combinations, APs whose SSIDs contain any combination of ruijie can be identified, such as RUIjie and RuiJie.
- Unless otherwise specified, configure a fuzzy containment keyword on devices requires this function.

Command	**countermeasures fuzzy-keyword** *string*
Parameter Description	*string*: Indicates the fuzzy containment keyword, which is case-insensitive and stored in lowercase.
Defaults	No fuzzy containment keyword is configured by default.
Command Mode	WIDS configuration mode
Usage Guide	The configuration takes effect only after the **countermeasures fuzzy-enable** command is executed. When the containment mode covers the SSID mode, rogue APs whose SSIDs contain the configured keyword will be contained. The fuzzy containment keyword takes effect only in SSID mode.

Enabling Unknown STA Detection and Containment

- Optional.
- Run the **device unknown-sta dynamic-enable** command to enable the unknown STA detection and containment function in WIDS configuration mode.
- Run the **device unknown-sta mac-address** *H.H.H* command to configure the unknown STA list entry in WIDS configuration mode.

Command	**device unknown-sta** { **dynamic-enable** | **mac-address** *H.H.H* | **mac-address max** *num* }
Parameter Description	**dynamic-enable**: Enables unknown STA detection and containment. **mac-address** *H.H.H*: Configures the unknown STA list entry, empty by default. **mac-address max** *num*: Configures the unknown STA list length, ranging from 1 to 256.
Defaults	Unknown STA detection and containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.
Command	**rogue-ap countermeasuresdevice unknown-sta report enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	The function takes effect only when the AP does not operate in Normal mode. The scanning result can be sent to the AC for display.

Configuring the Maximum Number of Detected APs

- Optional. Run the **device detected-ap-max** *num* command to configure the maximum number of detected APs in WIDS configuration mode. A smaller configuration value leads to less data being detected on the AP. If less data is detected, the device containment function may not show an obvious containment effect. A larger configuration value requires more memory.
- Unless otherwise noted, configure this on devices which need the maximum number of detected APs.

Command	**device detected-ap-max** *num*
Parameter Description	*num*: Indicates the maximum number of detected APs, ranging from 1 to 4,096.
Defaults	The default maximum number is 2,048.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Scanning Status of a Specified Radio

- Optional. Run the **hybrid-scan radio** *num* { **disable | enable** } command to configure the scanning status of a specified radio in AP configuration mode. If disabling the configuration leads to AP working in non-normal mode, there will be no device detection data.
- Unless otherwise noted, configure this on devices which need the radio scanning status.

Command	**hybrid-scan radio** *num* { **enable	disable** }
Parameter Description	*num*: Indicates a radio ID.
Defaults	All radio scanning is enabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Scanning Channel of a Specified AP

- Optional. Run the **scan-channels** { **802.11a** | **802.11b** } **channels** *num1 num2...num13* command to configure the scanning channel in AP configuration mode. If the scanning channel is not configured, there will be no device detection data when the AP operates not in Normal mode.
- Unless otherwise noted, configure this on devices which need the specified AP scanning channel.

Command	**scan-channels** { **802.11a**	**802.11b** } **channels** *num1 num2...num13*
Parameter Description	*num*: Indicates a channel number.
Defaults	The scanning channel is null.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Automatic Channel Scanning Between Different Frequency Bands

- Optional. Run the **scan-channels** { **dual-band** | **all-band** } **radio** *radio-id* command to perform automatic channel scanning among multiple frequency bands, to obtain the scanning result these frequency bands and perform containment.

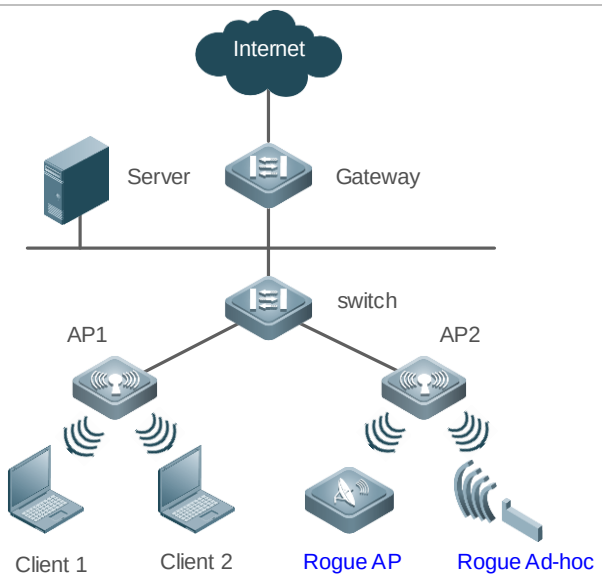
Command	**scan-channels dual-band radio** *radio-id*
Parameter Description	*radio-id*: Indicates the radio ID of the AP for which automatic channel scanning between different frequency bands is enabled.
Defaults	Automatic channel scanning between different frequency bands is disabled by default.
Command Mode	AP configuration mode
Usage Guide	The RF modules of partial APs support multiple frequency bands. When the RF modules are used for channel scanning, this command can be used for automatic channel scanning among multiple frequency bands, to obtain the scanning results of these frequency bands and perform containment. After the frequency bands are switched, channels configured by running the **scan-channels** { **802.11a**	**802.11b**	**6GHz** } **channels** command are scanned. Dual-band scans only 2.4 GHz and 5 GHz radios while all-band scans all radios supported by the AP. In addition, for some APs that have channel restrictions, the restricted channels will be automatically skipped during channel scanning.

Verification

- Run the **show wids detected** command to display the detected results.

Configuration Example

↘ Configuring Rogue Containment

Scenario	
Figure 1-8	
Configuration Steps	- Configure Rogue containment information on the device. Before configuring containment, confirm that the WLAN service has been deployed on the contained AP; otherwise, the containment will not take effect.

	Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# countermeasures enable Hostname(config-wids)# countermeasures mode ssid
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA and the log information generated by the system recently.
	Hostname#show running-config ... ! wids countermeasures enable countermeasures mode SSID ! ...

Common Errors

N/A

1.4.5 Configuring AP Working Mode

Configuration Effect

- Based on the configured working mode, the AP can provide different services.

Notes

N/A

Configuration Steps

↘ Configuring AP Working Modes

- Optional.
- Unless otherwise noted, configure this on each AP.

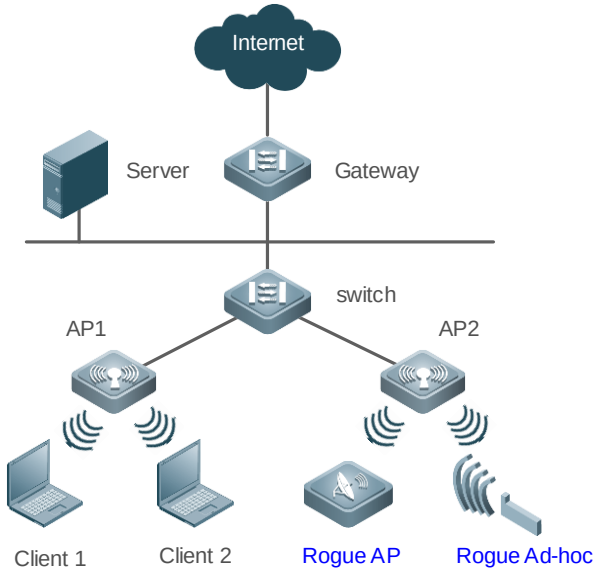
Command	**device mode** { **hybrid** | **monitor** [**radio** *radio-id*] | **normal** }
Parameter Description	**hybrid**: Indicates Hybrid mode, in which the device provides both monitoring service and access service. **monitor:** Indicates Monitor mode, in which the device provides only the monitoring service. **normal**: Indicates Normal mode, in which the device provides only the access service. *radio-id*: Specifies a radio to provide the monitoring service, while other radios to provide the access service.
Defaults	The working mode of the AP is Normal.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the current working mode of the AP.

Configuration Example

↘ Configuring the AP Working Mode

Scenario **Figure 1-9**	
Configuration Steps	• Configure the working mode of a specified AP. Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# device mode hybrid
Verification	• Run the **show running** command to display the information on related parameters configured by the STA. Hostname#show running ! wids device mode hybrid !

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the entries in the static attack list.	**reset attack-list all**
Clears the entries in the SSID-based blocklist.	**reset black-ssid all**
Clears the information of a specified device that is detected.	**reset detected { all | adhoc | rogue { ap | client } | mac-address H.H.H }**

Clears the entries in the dynamic blocklist.	**reset dynamic-blacklist { all | mac-address H.H.H }**
Clears the configuration of fuzzy containment keywords.	**reset fuzzy-keyword all**
Clears the entries in the allowed MAC list.	**reset permit-mac all**
Clears the entries in the allowed SSID list.	**reset permit-ssid all**
Clears the entries in the allowed vendor list.	**reset permit-vendor all**
Clears all or specified entries in the SSID-based blocklist and allowlist.	**reset ssid-filter { ssid all | in-ssid ssid }**
Clears all or specified entries in the SSID-based blocklist.	**reset ssid-filter { blacklist all | in-ssid ssid }**
Clears all or specified entries in the SSID-based allowlist.	**reset ssid-filter { whitelist all | in-ssid ssid }**
Clears the entries in the static blocklist.	**reset static-blacklist all**
Clears the information of the static attack statistic list.	**reset statistic all**
Clears the entries in the unknown STA list.	**reset unknown-sta all**
Clears the entries in the allowed list for user isolation.	**reset user-isolation-permit-list all**
Clears the entries in the allowlist.	**reset whitelist all**

Displaying

Description	Command
Displays the configuration of the attack list.	**show wids attack-list**
Displays the configuration of the dynamic and static blocklists.	**show wids blacklist** { **dynamic** | **static** }
Displays the configuration of the SSID-based blocklist.	**show wids black-ssid**
Displays the information of a specified device that is detected.	**show wids detected** { **adhoc** | **all** | **friendly ap** | **interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }

Configuring RF Management

1. Configuring Band Select
2. Configuring HE Radio Selection
3. Configuring RF Scheduling
4. Configuring Wireless Location

1 Configuring Band Select

1.1 Overview

Band Select is a technology for optimizing access band distribution for STAs on a WLAN.

The Band Select function leads dual-radio STAs to access the higher-capacity 5 GHz band and improve user experience.

The Band Select function is suitable for the following scenario: dual-radio APs are used to provide coverage, and the multiple RF connectors of the APs operate at 2.4 GHz, 5 GHz, and 6 GHz respectively; meanwhile, a WLAN is mapped to multiple RF connectors of the APs and provides access service at the multiple radio simultaneously.

Protocols and Standards

- IEEE 802.11

1.2 Applications

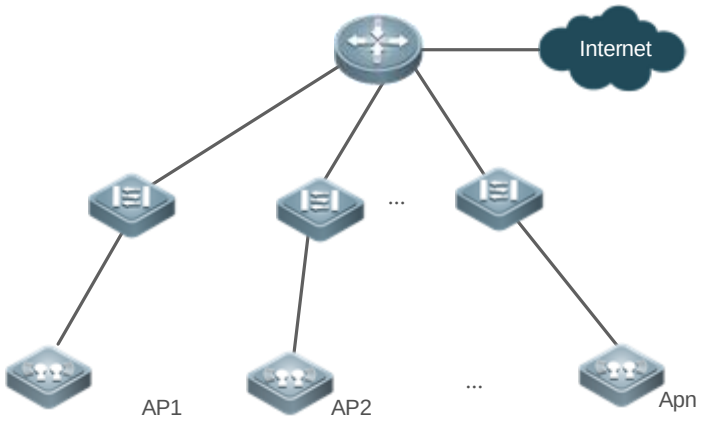
Application	Description
Enabling the Band Select Function on the Fat AP WLAN	A WLAN composed of multiple multi-band APs is enabled with the Band Select function.

1.2.1 Enabling the Band Select Function on the Fat AP WLAN

Scenario

WLAN signals are mapped to the RF connectors of all multi-radio APs.

Figure 1-1



Note: AP_1, AP_2 ... AP_n are multi-band APs.

Deployment

Enable the Band Select function on the APs to identify the STA types and guide the dual-radio STAs to access the 5 GHz band.

1.3 Features

Basic Concepts

IEEE802.11 Communication Band

IEEE802.11 comprises three radios:

- 2.4 GHz (2.412 to 2.4835 GHz) (IEEE 802.11b/g operates in this frequency band)
- 5 GHz (5.15 to 5.35 and 5.725 to 5.825 GHz) (IEEE 802.11a operates in this frequency band)
- 6 GHz (5925 MHz to 7125 MHz) (IEEE 802.11ax operates in this frequency band)

With the popularization of WLAN, most clients are capable of both 2.4 GHz and 5 GHz radios. The publish of Wi-Fi 6E standard ushers in the brand new 6 GHz radio, which is supported by many countries worldwide. The 6 GHz radio provides 59 available channels, 5 GHz radio provides 25 available channels, and 2.4 GHz radio provides 3 non-overlapping channels. The wireless clients should be steered to the 6 GHz and 5 GHz radios preferentially which offer a greater access capacity.

STA Scanning

There are two modes, namely, passive scanning and active scanning.

- Passive scanning: An STA monitors beacon frames sent by nearby APs on all channels of all supported bands. The beacon frames contain WLAN access information. The STA parses the information to learn about the WLANs that are available nearby.
- Active scanning: The STA broadcasts a Probe Request frame on all channels of all supported bands. After receiving the Probe Request frame, the APs providing WLAN access service sends a Probe Response frame including some WLAN information to the STA.

Generally, the STA summarizes the SSIDs of all discovered WLANs and provides an accessible WLAN list for users.

Multi-Band STA

WLAN network interface cards (WNICs) used by STAs to connect to WLANs are classified into a, b, g, n, ac, and ax, which indicate the 802.11 protocol types supported by the WNICs. 802.11a operates at 5 GHz, 802.11b/g at 2.4 GHz, 802.11n at 5 GHz and 2.4 GHz, 802.11ac at 5 GHz, and 802.11ax at 2.4 GHz, 5 GHz, and 6 GH.

Identify the frequency bands supported by the NIC according to the 802.11 specifications of the NIC.

Multi-Band AP

A multi-band AP requires multiple RF connectors working at the 5 GHz, 2.4 GHz, and 6 GHz radios respectively.

To enable a WLAN for band steering, map the WLAN to multiple RF connectors on the multi-band AP and enable access service at each radio.

Overview

Feature	Description
Identifying STA Types	The Band Select function identifies whether an STA is a multi-band STA.
Controlling the Active Scanning Process	The Band Select function controls active scanning of the multi-band STA to prevent the STA from discovering WLANs of the 2.4 GHz band.
Rejecting Accessing the 2.4 GHz Band	The Band Select function rejects the multi-band STA from accessing the 2.4 GHz band and improves the chance of accessing the 5 GHz band and 6 GHz band.

1.3.1 Identifying STA Types

To lead a multi-band STA to access the 5 GHz or 6 GHz radio, you should first identify whether the STA is a multi-band STA; that is, identify the band supported by the STA.

Working Principle

Active scanning is an approach for an STA to discover WLANs. When using active scanning, the STA sends a Probe Request frame on each supported channel. If the channel information in the Probe Request frame sent by the STA can be obtained, the bands supported by the STA can be identified.

For example, if an AP receives the Probe Request frame from the 2.4 GHz radio, the AP learns that the STA supports the 2.4 GHz radio. If the AP receives the Probe Request frame from the 5 GHz radio, the AP learns that the STA supports the 5 GHz radio. If the AP receives the Probe Request frame from the 6 GHz radio, the AP learns that the STA supports the 6 GHz radio.

Since a single-band AP can receive the Probe Request frame only at one band, only a multi-band AP can correctly identify the STA type. This is why the Band Select function requires a multi-band AP be used.

↘ STA Classification Standards

A multi-band AP classifies STAs based on the following standards:

- If the AP can receive the Probe Request frame from the 2.4 GHz, 5 GHz, and 6 GHz radios, this STA is a tri-radio STA.
- If the AP can receive the Probe Request frame from the 2.4 GHz and 5 GHz radio or from the 5 GHz and 6 GHz radio, the AP learns that this STA is a dual-radio STA.
- If the AP can receive the Probe Request frame from the 6 GHz radio, the AP learns that this STA is a 6 GHz STA.
- If the AP can receive the Probe Request frame from this STA only at the 5 GHz band, the AP learns that this STA is a 5 GHz STA.
- If the AP can receive the Probe Request frame from this STA only at the 2.4 GHz band, the AP learns that this AP is a 2.4 GHz STA.

The AP must wait for a period of time to verify that no Probe Request frame is received at the band; therefore, identifying a single-band STA is time-consuming but does not affect the normal use by users. Among the five types of STAs, the first two types are called the multi-band STAs and the last three type is called the single-band STAs.

It takes a period of waiting time (fixed to 2 seconds) to determine whether a Probe Request frame is sent from all radios. Due to different STA drivers, this time is not applicable to all multi-band STAs. Therefore, STA types may not be correctly identified in the beginning. As long as multi-band STAs can send Probe Request frames from all radios, the correct STA types can be identified.

STA Information Saving

The STA information identified by a multi-band AP must be saved to provide the basis for subsequent responding policies.

Since Probe Request frames sent by STAs are broadcast packets, an AP may receive many Probe Request frames generally. It is unnecessary to save all the frames because some distant STAs may not access the AP. Therefore, the Band Select function saves only the information of STAs that may have access. The selection criterion is the Received Signal Strength Indication (RSSI) of STAs. Only the RSSI exceeds a threshold can access the AP, and only then does the identified information need to be saved.

STA Information Aging

Users can configure the bands supported by some STAs; therefore, STA type may change during use.

Take an 802.11a/g/n-supported WNIC for example. The WNIC works as a dual-band STA in the beginning. However, a user disables its 802.11a mode or the support for the 5 GHz channels. Then, the WNIC changes to a single-band 2.4 GHz STA.

In this case, an aging mechanism needs to be used for the identified STA information. After a period of time, the previously identified STA information is discarded.

1.3.2 Controlling the Active Scanning Process

After identifying the bands supported by an STA, a multi-band AP can control the active scanning of the STA according to the STA information. The purpose is to prevent a multi-band STA from discovering 2.4 GHz WLANs and thus lead the multi-band STA to access the optimal band.

Working Principle

During active scanning, the STA broadcasts a Probe Request frame. After receiving the Probe Request frame, an AP sends a Probe Response frame immediately to inform the STA of the accessible WLANs on this AP. During active scanning of a multi-band STA, the STA sends a Probe Request frame and waits for a Probe Response frame on the multiple bands. After the Band Select function is enabled, the AP controls the active scanning and adopts different response approaches according to actual situations.

Active Scanning Before the Band Select Function Identifies STA Types

If the Band Select function is enabled for a WLAN, the WLAN may have different responses to active scanning of an STA. Before STA types are identified:

- The AP does not respond to Probe Request frames from the 2.4 GHz band.
- The AP responds to Probe Request frames from the 5 GHz and 6 GHz band.

After receiving a Probe Request frame from the 2.4 GHz band, the AP cannot determine whether the STA supports the 5 GHz and 6 GHz band. To prevent the STA from discovering that the WLAN provides access service at the 2.4 GHz band, the AP responds after the identification process ends.

If the AP receives a Probe Request frame from the 5 GHz and 6 GHz band, it indicates that the STA supports the 5 GHz and 6 GHz band. In this case, the AP sends a Probe Response frame immediately to tell the STA that WLAN provides access service at the 5 GHz and 6 GHz band.

↘ Active Scanning After the Band Select Function Identifies STA Types

When the AP receives a Probe Request frame after identifying the STA type, the AP can find the source MAC address in the Probe Request frame stored on the AP.

- If the STA is a multi-band STA, the AP does not respond to a 2.4 GHz Probe Request; if the STA is an inhibition STA, the AP responds negatively
- The AP responds to a 5 GHz and 6 GHz Probe Request.

Not responding to a 2.4 GHz Probe Request sent by a multi-band STA can prevent the multi-band STA from discovering that a WLAN provides access service at the 2.4 GHz band. In this way, the multi-band STA only discovers that the WLAN provides access service at the 5 GHz and 6 GHz bands. The multi-band STA has to select the 5 GHz and 6 GHz bands for access.

The AP must responds to the 2.4 GHz Probe Request from an inhibition STA. Since an inhibition STA supports only the 2.4 GHz band, the inhibition STA cannot identify a WLAN if the AP does not respond to the 2.4 GHz Probe Request. However, the response to an inhibition STA is negative.

A 5 GHz and 6 GHz Probe Request is sent only by a multi-band STA. Therefore, the AP must send a Probe Response immediately to tell the WLAN to provide access service at the 5 GHz band.

↘ Negative Response to an Inhibition STA

The Band Select function always positively responds to 5 GHz and 6 GHz Probe Requests, does not respond to 2.4 GHz Probe Requests sent by multi-band STAs, and responds to Probe Requests from inhibition STAs negatively. Figuratively speaking, a negative response is a discounted response. For example, when receiving multiple Probe Requests consecutively, the AP sends only one Probe Response.

The negativity depends on two parameters: STA scanning cycle threshold and the probe count of the inhibition STA.

- STA scanning cycle threshold

The STA scanning cycle indicates the time used to scan all supported channels during STA active scanning. Subject to the drivers of STAs, the cycle varies with different STAs.

The STA scanning cycle threshold can be configured by users and indicates the minimum value. If the scanning cycle of an STA is smaller than the threshold, two consecutive scanning cycles are considered as one by an AP. This parameter is useful when some STAs send multiple Probe Requests within one scanning cycle.

Example: Assume that an STA scans all channels every 150 milliseconds and sends two Probe Request frames consecutively on each channel. If an AP does not specify the minimum scanning cycle of the STA, the AP cannot identify whether the STA sends two frames within the same scanning cycle or sends the two frames in two consecutive scanning cycles. If the AP sets the minimum scanning cycle of the STA to 200 milliseconds, the two frames are considered to be sent within the same scanning cycle because their interval is shorter than 200 milliseconds. The probe count of the STA on the AP is 1. Since the specified minimum scanning cycle (200 milliseconds) and the actual scanning cycle (150 milliseconds) are different, the counts are also different. Assume that the STA performs scanning for three consecutive cycles, the count on the AP will be 2 because the first two cycles are considered to be one. However, this problem does not cause inconvenience to users.

- The probe count of the inhibition STA

The probe count of an inhibition STA reflects the negative response degree of a HE RF connector to an STA. This parameter indicates the number of the cycles for which an inhibition STA performs active scanning before an AP sends one response. For example, if the default value is 2, the STA performs scanning for two consecutive cycles before the AP sends a Probe Response frame.

1.3.3 Rejecting Accessing the 2.4 GHz Band

⚠ The Band Select function controls only the active scanning of an STA, but cannot prevent the STA from discovering a 2.4 GHz WLAN through passive scanning. Therefore, some multi-band STAs can still discover 2.4 GHz WLANs and attempt to access the WLANs. In this case, the Band Select function may fail.

The Band Select function can reject 2.4 GHz access requests from multi-band STAs to improve the chance for multi-band STAs accessing the 5 GHz and 6 GHz bands.

⚠ Rejecting a multi-band STA's 2.4 GHz access request helps facilitate the Band Select function; however, the Band Select function cannot be 100% successful.

Working Principle

After an STA discovers a WLAN for a user to access the WLAN, the STA sends an Authentication Request to the AP at first. Then, the AP sends an Authentication Response to permit or reject the STA's authentication request.

The Band Select function processes the Authentication Request. If the Authentication Request is sent by a multi-band STA at the 2.4 GHz band, the function can reject the Authentication Request until the multi-band STA sends an Authentication Request from the 5 GHz or 6 GHz band. Thus, the STA is led to access the 5 GHz or 6 GHz band.

Generally, when a multi-band STA searches for access, the STA sends one or more Authentication Requests at a band and waits for responses. If the STA does not receive responses or fails in access, the STA sends Authentication Requests at the other band and waits for responses. However, some multi-band STAs send Authentication Requests only at the 2.4 GHz. For high availability, you can use the Band Select function to set the rejecting count for a multi-band STA.

Assume that a multi-band STA sends Authentication Requests for M times before changing the band, and the rejecting count is set to N. If the multi-band STA attempts to access the 5 GHz band at first, the STA can access the 5 GHz or 6 GHz band immediately. If the multi-band STA attempts to access the 2.4 GHz band at first, the STA can access the 5 GHz or 6 GHz band only if N is equal to or greater than M; otherwise, the STA accesses the 2.4 GHz band. No matter which band a multi-band STA accesses, if the multi-band STA attempts to access the 2.4 GHz band at first, min (smaller one between M and N) Authentication Requests are rejected or ignored. As a result, the STA's access is delayed. The delay time depends on the driver of the STA. For example, if the STA sends Authentication Requests at the interval of 100 milliseconds and four Authentication Requests are ignored, the access of the STA will be delayed for 400 milliseconds.

⚠ When the Band Select function rejects the access request of a multi-band STA while another access control module such as load balance accepts the access request, the STA will still gain access. This is

because the Band Select function plays only the "leading" role during STA access and has a low priority. When the Band Select function conflicts with other functions, the other functions shall prevail.

1.4 Configuration

Configuration	Description and Command	
Configuring Band Select	⚠ (Mandatory) It is used to enable the Band Select function for a WLAN.	
	band-select enable	Enables the Band Select function.
	⚠ (Optional) It is used to set the parameters of the Band Select function.	
	band-select acceptable-rssi	Configures the minimum RSSI for the Band Select function.
	band-select access-denial	Configures the rejecting count for a multi-band STA's 2.4 GHz access requests.
	band-select age-out	Configures the aging time of STA information.
	band-select probe-count	Configures the probe count of an inhibition STA.
	band-select scan-cycle	Configures the scanning cycle threshold of an STA

1.4.1 Configuring Band Select

Configuration Effect

- Enable the Band Select function for a WLAN to lead multi-band STAs to access the 5 GHz or 6 GHz band.

Notes

- N/A

Configuration Steps

↘ Enabling the Band Select Function for a WLAN

- Mandatory.
- If there is no special requirement, enable this function on a fat AP.

Command	band-select enable
Parameter Description	N/A
Defaults	The Band Select function is disabled.
Command	WLAN configuration mode

Mode	
Usage Guide	N/A

Configuring the Minimum RSSI for the Band Select Function

- (Optional) It is configured when you want to adjust the coverage of the Band Select function.
- If there is no special requirement, enable this function on a fat AP.
- The higher the value, the smaller the coverage of the Band Select function; the lower the value, the larger the coverage of the Band Select function. However, if the value exceeds a certain limit, the STA signals that gain access may be too weak, causing the connection rate of the entire network to slow down.

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Specifies the minimum SSID for the Band Select function, ranging from -100 to -50 dBm.
Defaults	The default value is -80 dBm
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Rejecting Count for a Multi-Band STA's 2.4 GHz Access Requests

- (Optional) It is configured when it is necessary to reject the 2.4 GHz access request of multi-band STAs. If many STAs fail in access or it takes much time to access, configure this parameter to a smaller value or to 0.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The more the rejecting count is, the more difficult the multi-band STA accesses the 2.4 GHz band, and the later the STA accesses the 2.4 GHz band. On the other hand, the less the rejecting count is, the easier the multi-band STA accesses the 2.4 GHz band, and the sooner the STA accesses the 2.4 GHz band.

Command	**band-select access-denial** *value*
Parameter Description	*value*：Specifies the rejecting count for a multi-band STA's 2.4 GHz access requests, ranging from 0 to 10.
Defaults	The default value is 2
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Aging Time of STA Information

- (Optional) If no multi-band STAs change to single-band 2.4 GHz STAs, configure a longer aging time. Otherwise, configure a shorter aging time. If it is uncertain, use the Defaults.
- If there is no special requirement, enable this function or a fat AP.

- The longer the STA information aging time, the longer the lifecycle of STA information, and the less sensitive of an AP to STA's band change. The shorter the STA information aging time, the shorter the lifecycle of STA information, and the more sensitive of an AP to STA's band change.

Command	**band-select age-out** { **dual-band** *value* | **suppression** *value* }
Parameter Description	**dual-band** *value*：Specifies the aging time of multi-band STA information, ranging from 20 to 120 seconds. **suppression** *value*: Specifies the aging time of inhibition STA information, ranging from 10 to 60 seconds.
Defaults	The aging time of multi-band STA information is 60 seconds and the aging time of inhibition STA information is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended that the aging time of multi-band STA information be set to twice or three times that of inhibition STA information.

Configuring the Probe Count of an Inhibition STA

- (Optional) If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value.
- If there is no special requirement, enable this function on a fat AP.
- The greater the probe count of an STA, the stronger inhibition the Band Select function performs on an inhibition STA, and the more difficult the inhibition STA discovers a WLAN. On the other hand, the smaller the probe count of an STA, the weaker inhibition the Band Select function performs on an inhibition STA, and the easier the inhibition STA discovers a WLAN.

Command	**band-select probe-count** *value*
Parameter Description	*value*: Specifies the probe count of an inhibition STA, ranging from 1 to 10.
Defaults	The default value is 2.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Scanning Cycle Threshold of an STA

- (Optional) If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value. If it is uncertain, use the Defaults.
- If there is no special requirement, enable this function on a fat AP.
- The greater the scanning cycle threshold of an STA, the more slowly the probe count of the STA increases, and the more difficult the STA discovers a WLAN. On the other hand, the smaller the scanning cycle threshold of the STA, the more quickly the probe count of the STA increases, and the easier the STA discovers a WLAN.

Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Specifies the scanning cycle threshold of an STA, ranging from 1 to 1000 milliseconds.
Defaults	The default value is 200 milliseconds.

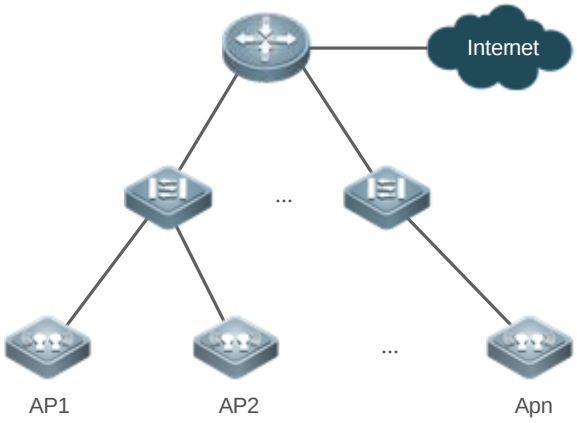
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show band-select configuration** command to display parameters of the Band Select function.
- Run the **show running-config** command to check whether the Band Select function is enabled.
- After a period of running, run the **show band-select statistics** command to check the statistics.
- Check whether the Band Select function controls the active scanning process by capturing packets.

Configuration Example

Enabling the Band Select Function on the Fat AP WLAN

Network Environment Figure 1-2	 The figure shows a WLAN with the fat AP architecture. ● AP1, AP2, ..., and APn are dual-radio APs. ● Multiple dual-radio APs are connected to Layer 2 switches and Layer 3 routers. ● The Band Select function is enabled on WLAN 1. The SSID is **wlan-bandselect** . The WLAN signal maps to the RF connectors of all dual-radio APs.
Steps	● (Optional) Configure the running parameters of the Band Select function. ● Enable the Band Select function on WLAN 1.
	Hostname# configure terminal Hostname(config)# dot11 wlan 1 Hostname(dot11-wlan-config)# band-select enable
Verification	Access WLAN "wlan-band select" by using a multi-band STA. ● The STA accesses the 5 GHz band. (A selection failure may occur. That is, the STA accesses 2.4 GHz band.) ● Check the Band Select running statistics on the AP. There should be a count increase.
	Hostname# show band-select statistics Band Select Statistics

	Number of dual band client..... 1 Number of dual band client added..... 1 Number of dual band client expired..... 0 Number of suppressed client..... 0 Number of suppressed client added..... 0 Number of suppressed client expired..... 0

Common Errors

- The parameters are improper.
- The Band Select function is not enabled.
- An RF connector of a multi-band AP is disabled.

1.5 Monitoring

Displaying

Description	Command
Displays the configuration of the Band Select function.	**show band-select configuration**
Displays the statistics of the Band Select function.	**show band-select statistics**

1 Configuring HE Radio Selection

1.1 Overview

High-efficiency (HE) radio selection chooses a HE radio frequency (RF) port on an access point (AP) based on the channel load and other conditions when multiple types of STAs coexist and enables HE STAs (HIGH-STAs for short) to preferentially access the HE RF port to obtain a better user experience on a Wi-Fi 6 AP.

Protocols and Standards

- IEEE 802.11

1.2 Applications

Application	Description
Configuring HE Radio Selection in the Fat AP Architecture	In the fat AP architecture with densely deployed tri-radio APs, Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6 STAs are distributed to radios at random. Low-speed STAs affect the user experience of Wi-Fi 6. The HE radio selection function leads HIGH-STAs to HE radios.

1.2.1 Configuring HE Radio Selection in the Fat AP Architecture

Scenario

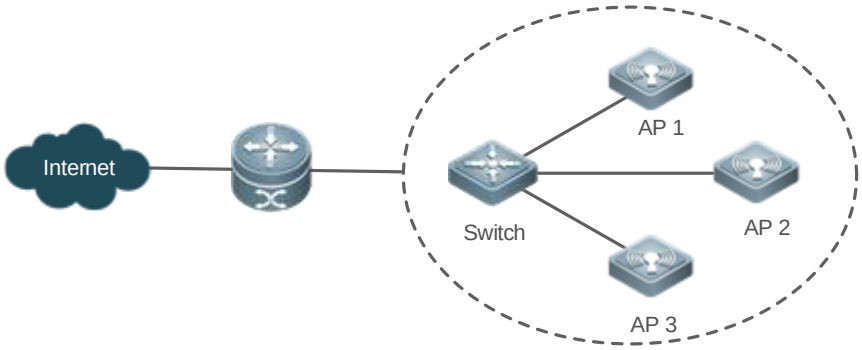
On a wireless local area network (WLAN) formed by multiple tri-radio APs in the fat AP architecture, a large number of Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6 STAs exist and the STAs may access APs at random. When low-speed STAs are used together with Wi-Fi 6 STAs, high throughput of Wi-Fi 6 STAs cannot be used. The HE radio selection function can lead HIGH-STAs to HE radios.

The HE radio selection function independently selects a HE radio and occupies it when both high-speed and low-speed STAs exist. If only low-speed or high-speed STAs exist, you are not advised to enable this function.

As shown in Figure 1-1,

- APs connect with the layer-3 router through a layer-2 switch.
- WLAN signals are mapped to the three RF ports of all tri-radio APs.

Figure 1-1



Remarks	AP1, AP2, and AP3 are tri-radio APs.

Deployment

- Manage and configure the working parameters of the HE radio selection function on the APs.
- Run the HE radio selection function on APs. Based on the RF environment of an AP, the HE radio selection function automatically selects a HE radio, identifies HIGH-STAs, and leads the HIGH-STAs to the HE radio.

1.3 Features

Basic Concepts

IEEE 802.11 Communication Radios

IEEE 802.11 main communication radios are classified as follows:

- 2.4 GHz (2.4 to 2.4835 GHz), radio where 802.11b/g/n/ax resides
- 5 GHz (5.15 to 5.35 GHz and 5.725 to 5.825 GHz), radio where 802.11a/n/ac/ax resides

With the popularization of WLAN, the number of wireless users increase, and most users use STAs that support both 2.4 GHz and 5 GHz. However, 802.11b/g is applied more widely than 802.11a. Many dual-band STAs use 2.4 GHz, which causes congestion at 2.4 GHz and resource waste at 5 GHz. In fact, 5 GHz has a larger access capacity than 2.4 GHz. 2.4 GHz can have three non-overlapped communication channels at most. 5 GHz can provide more non-overlapped communication channels.

WLAN Discovery by STAs

STAs discover a WLAN through passive scanning or active scanning.

- Passive scanning: An STA monitors the Beacon frames sent by nearby APs in all channels of all supported frequency bands. A Beacon frame contains a WLAN that provides the access service and additional information. The STA can parse the information to understand the accessible WLANs nearby.
- Active scanning: An STA broadcasts a probe request frame in all channels of all supported frequency bands. When an AP that provides the WLAN access service receives the probe request frame, the AP sends the WLAN information to the STA in a probe response frame.

Generally, the STA summarizes the service set identifiers (SSIDs) of all discovered WLANs and displays the list of accessible WLANs for the user to select.

↘ HIGH-STA

With the emergence of Wi-Fi 6 and promotion of tri-radio APs, the user experience of HIGH-STAs is easily affected when wireless STAs are associated with radios on APs at random, HIGH-STAs that support 802.11ac/802.11ax access 2.4 GHz RF ports, or a large number of low-speed STAs occupy air interface resources of a radio. For STAs that support 802.11ac/802.11ax, the HE radio selection function can be used to lead these STAs to HE RF ports.

↘ Dual-5G AP

Dual-5G APs can access two 5 GHz frequency bands simultaneously. The corresponding tri-radio APs need to support dual-5G coverage. Signals of a WLAN with HE radio selection enabled must be mapped to the three RF ports of all tri-radio APs, and all the three RF ports provide access service to STAs.

Overview

Feature	Description
Identifying the STA Type	Identifies whether an STA is a HIGH-STA. (STAs that support 802.11ax are identified as HIGH-STAs by default, which is configurable.)
Automatically Selecting a HE Radio	Automatically selects a HE radio based on the RF environment load and interference of an AP.
Controlling Active Scanning	Controls active scanning of different types of STAs to prevent non-HIGH-STAs from discovering WLAN signals of HE radios.
Rejecting STAs	Identifies the type of STAs and rejects HIGH STAs to non-HE radios. Identifies the type of STAs and rejects non-HIGH STAs to HE radios.
Automatically Adjusting the Selection Policy Based on the Radio Status	Automatically adjusts the selection policy based on the radio status.

1.3.1 Identifying the STA Type

Before the HE radio selection function takes effect, an AP needs to identify whether an STA is a HIGH-STA, that is, check whether an STA supports HT_CAP.

Working Principle

Active scanning is a method for an STA to discover a WLAN. When an STA uses active scanning, it sends a probe request frame to each supported channel. If the HT/VHT/HE information can be identified from the 802.11 field carried in the probe request frame sent by the STA, protocols supported by the STA can be identified.

↘ STA Classification Standard

An AP classifies STAs based on the following standard:

- HT-STAs: STAs that support 802.11a/b/g/n
- VHT-STAs: STAs that support 802.11ac
- HE-STAs: STAs that support 802.11ax

- Non-HIGH-STA:

  When an STA accesses an AP, the AP parses the probe request and assoc request packets to confirm the capabilities supported by the STA. Based on the types of HIGH-STAs specified by HE radios in the delivered configuration, the AP classifies STAs and defines non-identified HIGH-STAs as non-HIGH-STAs.

⚠ STA identification depends on the probe request and assoc request packets. However, in the authentication phase, the packets cannot be parsed.

STA Information Saving

STA information identified by an AP needs to be saved to provide a basis for subsequent response policies.

Because STAs broadcast probe requests, an AP will receive many probe requests. It is unnecessary to save all the requests because some STAs that are far away from the AP are impossible to access the AP. Therefore, the HE radio selection function only saves information about the STAs that may access the AP based on the received signal strength indicator (RSSI). Only the STAs whose RSSI exceeds a threshold may access the AP and whose information needs to be saved.

STA Information Aging

Users can configure the frequency bands supported by STAs. When an STA accesses the network, the frequency bands supported by the STA may be changed. In addition, more and more STAs support the random media access control (MAC) address function. Therefore, the STA information aging mechanism is introduced.

For example, a wireless network interface card (NIC) that supports 802.11ax is a HIGH-STA that supports 802.11ac/ax when it is used. When the user manually disables the 802.11ac/ax mode, the NIC is changed to a non-HIGH-STA that supports 802.11n.

In this situation, the aging mechanism is required for identified STA information. After a period of time, previously identified STA information needs to be discarded and STA information needs to be re-identified.

1.3.2 Automatically Selecting a HE Radio

The HE radio selection function needs an AP to support dual-band 5G and use a HE radio with small interference. After the HE radio selection function is enabled, the AP can automatically select a radio with a light load and low interference based on the current channel environment to ensure the user experience of HIGH-STAs.

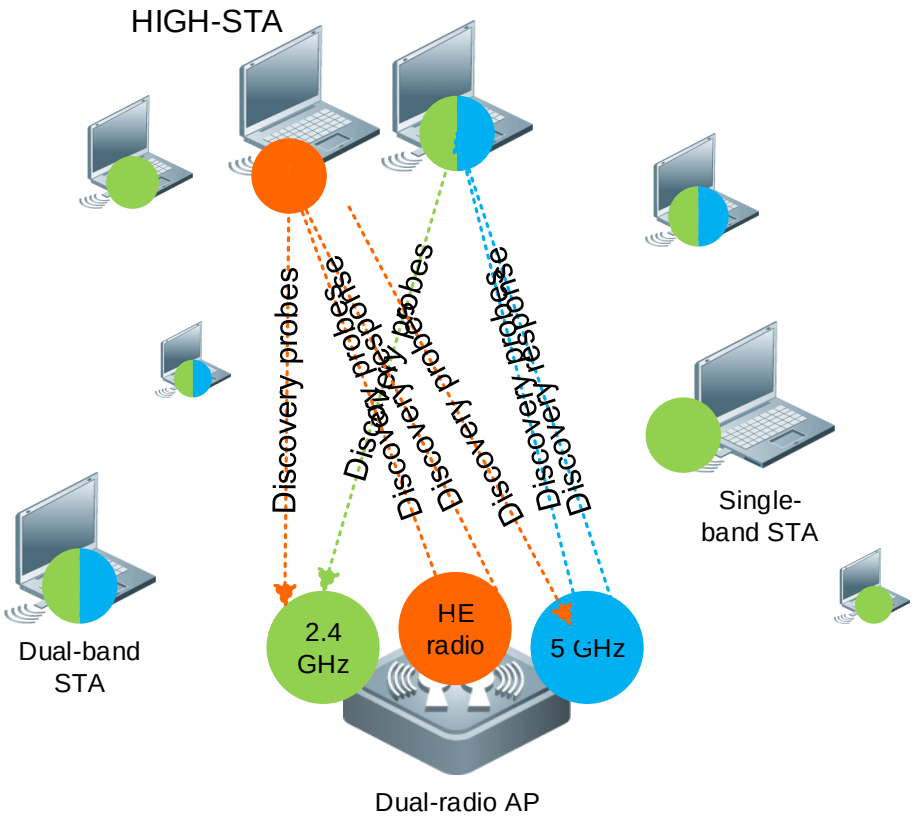
1.3.3 Controlling Active Scanning

After identifying the capabilities supported by an STA, a tri-radio AP can control active scanning of the STA. This prevents HIGH-STAs from discovering signals of non-HE radios and leads HIGH-STAs to access 5 GHz. In addition to preventing HIGH-STAs from discovering signals of non-HE radios, the AP needs to prevent non-HIGH-STAs from accessing HE radios to ensure the air interface efficiency of HE radios.

Working Principle

During active scanning, an STA broadcasts a probe request frame. After an AP receives the frame, it responds with a probe response frame and tells the STA the signals on the AP that can provide the access service. During active scanning, an STA sends a probe request to both frequency bands and waits for a probe response. After

the HE radio selection function is enabled, the AP needs to control response to active scanning and adopts different response methods in different scenarios.



Response of HE Radio Selection to Active Scanning of STAs

If HE radio selection is enabled on an AP, response to active scanning of an STA will be changed. After identifying STA capability information:

✓ HE radios

- The AP does not respond to probe requests from non-HIGH-STAs
- but respond to probe requests from HIGH-STAs.

✓ Non-HE radios

- The AP responds to probe requests from non-HIGH-STAs
- but does not respond to probe requests from HIGH-STAs.

Negative Response of HE Radio Selection to Non-HIGH-STAs

HE RF ports actively respond to probe requests from HIGH-STAs and do not respond to probe requests from non-HIGH-STAs. Non-HE RF ports negatively respond to probe requests from HIGH-STAs. That is, non-HE RF ports only respond with one probe response after receiving multiple consecutive probe requests.

The negative response degree of HE radio selection to probe requests from STAs depends on two parameters: STA scanning period threshold and STA probe scanning period count.

- STA scanning period threshold

  The STA scanning period indicates the time for scanning all supported channels during STA active scanning, and the time varies depending on the STA. The STA scanning period threshold is a configurable value and

indicates the minimum value for the STA scanning period. If the STA scanning period is less than the value, the AP regards two consecutive scanning periods as one scanning period. An STA may send multiple probe request frames in one scanning period.

For example, an STA scans all channels every 150 ms and sends two consecutive probe request frames on each channel. If the minimum value of the STA scanning period is not specified on the AP, the AP cannot determine whether an STA sends two probe request frames in one scanning period or one probe request frame in two consecutive scanning periods, respectively. If the minimum value of the STA scanning period configured on the AP is 200 ms and the interval between two packets is less than 200 ms, the AP regards that the packets are sent from the same scanning period and the scanning period count of the STA on the AP is 1. Because the minimum value of the STA scanning period specified on the AP is 200 ms, which is different from the actual scanning period of 150 ms, inconsistent counts may exist. When an STA has three scanning periods, only two periods are counted on the AP because the AP regards the previous two periods as one period.

- STA scanning period count

  The STA scanning period count reflects the negative response degree of a HE RF port to an STA. The count indicates the number of STA active scanning periods that an AP sends a response. For example, the default value of the count is 2. It indicates that the AP gives a probe response frame after two consecutive scanning periods of an STA.

1.3.4 Rejecting STAs

⚠ The HE radio selection function only controls the active scanning process of an STA and cannot prevent the STA from discovering signals of non-HE radios through passive scanning. Therefore, some HIGH-STAs can discover signals of non-HE radios and try to access. In this case, the HE radio selection function becomes invalid.

After the HE radio selection function is enabled, non-HE radios can reject access requests from HIGH-STAs to improve the success rate for HIGH-STAs to access HE radios. In addition, HE radios can reject access requests from non-HIGH-STAs to maintain high-speed throughput of air interfaces of HE radios.

⚠ Rejecting access requests from HIGH-STAs in non-HE radios can improve the success rate of HE radio selection but cannot reach 100%. HE radio selection may be invalid.

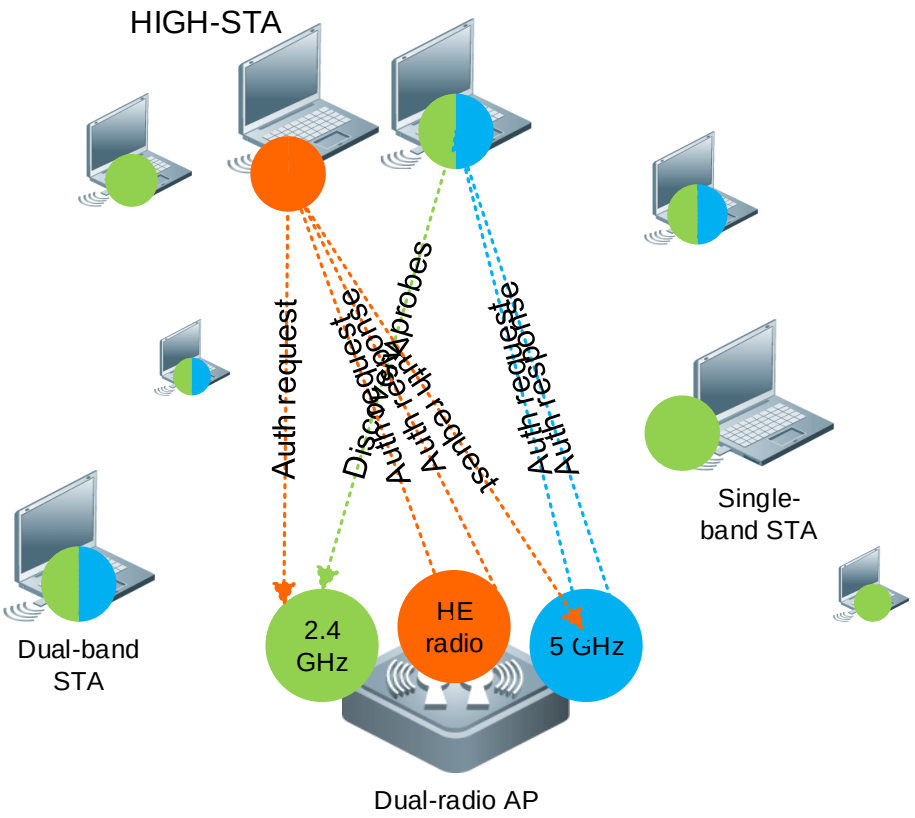
Working Principle

After an STA discovers and accesses a WLAN, the STA first sends an authentication request to an AP. The AP responds with an authentication response to allow or reject the authentication request of the STA.

The HE radio selection function can process authentication request frames. When a non-HIGH-STA sends an authentication request to a HE radio, the HE radio can reject its authentication request until it receives an authentication request from a HIGH-STA. This leads tri-band STAs to access HE radios.

When a HIGH-STA accesses the network, it sends one or multiple authentication requests in a frequency band and waits for a response. If no response is received or the authentication request fails to be sent, the STA transfers to another frequency band to send an authentication request and waits for a response. However, a

HIGH-STA may send authentication requests only in non-HE radios. To ensure high availability, HE radio selection can configure the number of times for rejecting access requests from non-HIGH-STAs.



For example, a HIGH-STA accesses the network and sends *M* authentication requests before switching to another frequency band, and the number of times that the HE radio selection function rejects access requests from a HIGH-STA is configured as *N*, the following situations exist:

- If the HIGH-STA first attempts to access a HE radio, the access is successful.
- If the HIGH-STA first attempts to access a non-HE radio, the following situations exist:

  1) If *N* is greater than or equal to *M*, the STA can access the HE radio.

  2) Otherwise, the STA accesses a non-HE radio.

  In this scenario, min (M, N) authentication requests will be rejected or ignored. Therefore, it takes a long time for some STAs to access the network. The delayed time varies depending on the STA. For example, an STA sends authentication requests every 100 ms and four authentication requests are ignored, network access of the STA will be delayed for 400 ms.

When the HE radio selection rejects the access request of a HIGH-STA but another access control module, such as load balancing accepts the access request of this STA, the STA is allowed to access. The HE radio selection function is only used to lead STAs during STA access and has a low priority. When the function conflicts with other functions, other functions preferentially take effect.

1.3.5 Automatically Adjusting the Selection Policy Based on the Radio Status

When the HE radio selection function is enabled, an extreme situation may occur in some scenarios. When there are a large number 802.11ax STAs or 802.11n low-speed STAs, some HE radios may not have STAs and a large number of 802.11ax STAs are centralized in a radio. As a result, the user experience on the radio is poorer than that in random association.

Working Principle

The AP will analyze STA access of HE radios and non-HE radios. Based on STA access and channel load of radios, the AP adjusts the selection policy to ensure an easy-to-use function.

1.4 Configuration

Configuration	Description and Command	
Configuring HE Radio Selection	(Mandatory) It is used to enable the HE radio selection function for a device.	
	band-optimize he-radio enable [**auto** | **fixed**]	Configures the HE radio selection function.
	band-optimize he-radio mode [**11axonly** | **11ac_11ax**]	Configures the type of STAs that access HE radios.
	(Optional) It is used to configure the working parameters of the HE radio selection function.	
	band-select acceptable-rssi	Configures the lower limit of the STA signal strength that the HE radio selection function can accept, which also applies to band selection.
	band-select he-radio access-denial	Configures the number of times for rejecting STAs to a radio.
	band-select age-out	Configures the aging time of STA information, which also applies to band selection.
	band-select he-radio probe-count	Configures the STA scanning period count.

1.4.1 Configuring HE Radio Selection

Configuration Effect

- Enable the HE radio selection function on an AP and lead HIGH-STAs to HE radios.

Notes

N/A

Configuration Steps

Enabling HE Radio Selection for an AP

- (Mandatory)
- Configure it in fat AP mode unless otherwise specified.

Command	band-optimize he-radio enable
Parameter Description	N/A
Defaults	The HE radio selection function is disabled by default.
Command Mode	Global configuration mode of APs
Usage Guide	

Configuring the Usage Mode of HE Radio Selection

- Optional. Configure it when HE radio selection needs to be adjusted in an environment.
- Configure it in fat AP mode unless otherwise specified.
- Enable the HE radio selection function.

Command	**band-optimize he-radio enable** [**auto** | **fixed**]
Parameter Description	**auto**: Automatically adjusts the selection policy based on the load usage of a radio. **fixed**: Forcibly navigate HIGH-STAs to HE radios when the HE radio selection function is enabled, which is not changed due to RF environment differences.
Defaults	**auto**
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Type of STAs That Access HE Radios

- Optional. Based on the STA distribution in the environment, specify the type of STAs that access HE radios.
- Configure it in fat AP mode unless otherwise specified.

Command	**band-optimize he-radio mode** { **11axonly** | **11ac_11ax** }
Parameter Description	**11axonly**: Leads only 802.11ax STAs to HE radios. **11ac_11ax**: Leads only 802.11ac and 802.11ax STAs to HE radios.
Defaults	The default mode is **11axonly**.
Command Mode	Fat AP: Global configuration mode
Usage Guide	N/A

Configuring the Number of Times That HE Radio Selection Rejects an STA

- Optional. Configure the number of times that a HE radio rejects authentication requests from a non-HIGH-STA or the number of times that a non-HE radio rejects authentication requests from a HIGH-STA.
- To prevent STAs from accessing non-matching radios, the number of times that HE radio selection rejects an STA needs to be set to a smaller value or 0 if multiple STAs access the network after a long time or cannot access the network.
- Configure it in fat AP mode unless otherwise specified.
- The larger the number of times that a radio rejects an STA, the more difficult and more time for the STA to access the radio.

Command	**band-select he-radio access-denial** *access-denial-time*
Parameter Description	*access-denial-time*: Number of reject times, ranging from 0 to 10.
Defaults	2
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Number of Times That the HE Radio Selection Function Suppresses an STA

- Optional. Configure the number of times that a HE radio rejects probe requests from a non-HIGH-STA or the number of times that a non-HE radio rejects probe requests from a HIGH-STA.
- Configure it in fat AP mode unless otherwise specified.
- A longer STA information aging time indicates a longer STA information lifecycle and less sensitive to radio switching of an STA. A shorter STA information aging time indicates a shorter STA information lifecycle and more sensitive to radio switching of an STA.

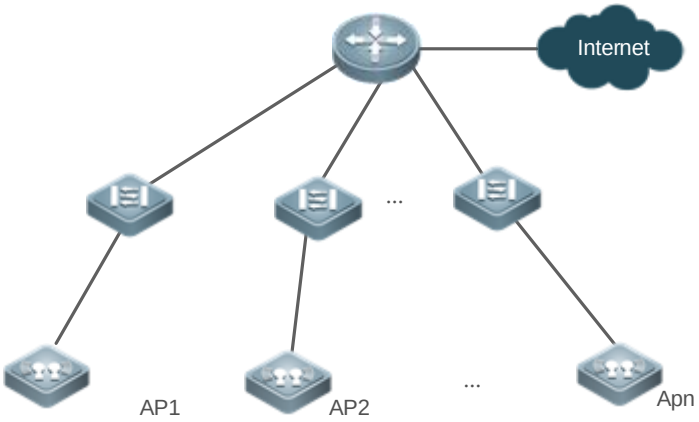
Command	**band-select he-radio probe-count** *probe-count*
Parameter Description	*probe-count*: Number of times that a non-HE radio rejects probe requests from a HIGH-STA, ranging from 0 to 10.
Defaults	2
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show band-select configuration** command
- to display HE radio selection parameter configuration on the device.
- Run the **show running-config** command to check whether the HE radio selection function is enabled in WLAN configuration.
- After a period of time, run the **show band-select statistics** command to display the running statistics on the device.
- Capture packets to confirm whether HE radio selection controls the active scanning process.

Configuration Example

Configuring HE Radio Selection for a Device

Scenario **Figure 1-2**	 The preceding figure shows a typical wireless network with the fat AP architecture. ● AP1, AP2, and AP3 are tri-radio APs. ● APs connect with the layer-3 router through a layer-2 switch. ● The HE radio selection function is enabled, the WLAN is WLAN 99, the SSID is wlan-bandoptimize, and the WLAN maps to three RF ports of all tri-radio APs.
Configuration Steps	● Configure HE radio selection running parameters (optional). ● Enable HE radio selection for WLAN 99.
	Hostname# configure terminal Hostname(config)# band-optimize he-radio enable
Verification	Use a HIGH-STA to access WLAN "wlan-bandselect". ● The STA accesses a HE radio. (Selection may fail, and the STA accesses a non-HE radio.) ● Check that the HE radio selection running statistics on the AP increase.
	Hostname# show band-select statistics Band Select Statistics Number of dual band client..... 1 Number of dual band client added..... 1 Number of dual band client expired..... 0 Number of suppressed client..... 0 Number of suppressed client added..... 0 Number of suppressed client expired..... 0 AP Name IP Address Radio 11n 11ac 11ax Radio 11n 11ac 11ax ---------- ---------- ---- ------ ----- ----- ----- --------- ----- ------ ------ AP-test 192.168.10.6 1# 3 4 0 2# 5 7 0 3#P 0 0 8 NA

Common Errors

- The HE radio selection running parameters are not configured properly.
- The HE radio selection function is disabled.
- One of the two 5G RF ports of a tri-radio AP is disabled.

1.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays HE radio selection running statistics.	**show band-select statistics**
Displays STA distribution to radios of an AP to display STA distribution of HE radios.	**show dot11 associations all-client** { *radio number* }

Debugging

N/A

1 Configuring RF Scheduling

1.1 Overview

The radio frequency (RF) resources mentioned in this document include the RF of an Access Point (AP) as well as a wireless local area network (WLAN) services.

RF scheduling can perform automatic management on the RF resources.

RF scheduling can be used to disable the RF of an AP or a WLAN in the specified time interval, realizing the following functions:

- Reducing network traffic, saving network resources, and preventing waste or abuse of network resources
- Reducing RF interference and saving energy
- Disabling access services in a certain period to reduce potential security risks

RF scheduling can be used in the scenarios where wireless access services are required in specific time cycles.

1.2 Applications

Application	Description
Configuring AP Radio Scheduling	AP radio scheduling can be used to enable or disable an AP radio at a scheduled time.
Configuring WLAN Scheduling	WLAN scheduling can be used to enable or disable a WLAN at a scheduled time.

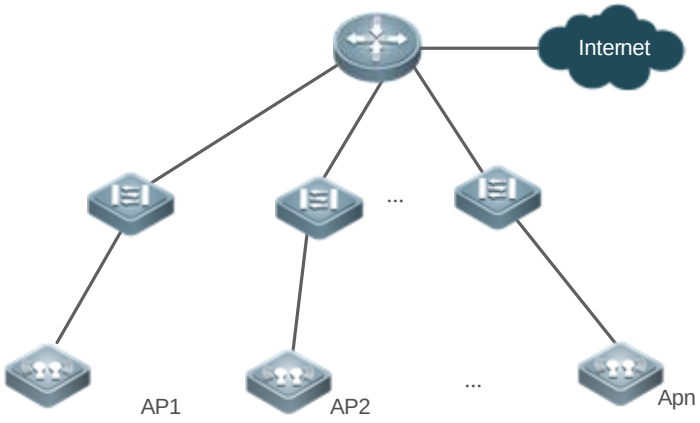
1.2.1 Configuring AP Radio Scheduling

Scenario

If STAs use wireless access services at a fixed time, AP radio scheduling can be configured to disable an AP radio when no STA accesses a WLAN. This saves network resources and electric power.

In the deployment scenario of a WLAN with the fat AP architecture, AP radio scheduling can be used to automatically disable an AP radio at night and enable an AP radio in the daytime when STAs need to access a WLAN. This guarantees normal WLAN services for STAs and saves network resources and energy at the same time.

Figure 1-1



Deployment

Configure AP radio scheduling on fat APs.

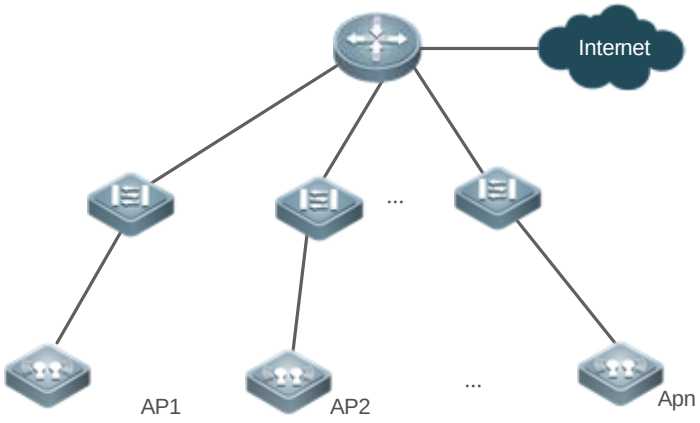
1.2.2 Configuring WLAN Scheduling

Scenario

Some special WLANs are enabled only when necessary, which reduces radio frequency interference and ensures security.

In the deployment scenario of a WLAN with the fat AP architecture, WLAN scheduling can be used to automatically enable WLAN services during the working hours of network administrators and disable WLAN services after network administrators get off work. At this time, free WLAN services are unavailable, but employees working overtime can access other WLANs.

Figure 1-2



Deployment

Configure WLAN scheduling on fat APs.

1.3 Features

Basic Concepts

Scheduling Session

A scheduling session indicates a time interval for an RF resource. A simple scheduling session contains only one time interval in a certain day; a complex scheduling session contains many duplicate time intervals in different dates. Currently, one scheduling session supports eight different (or same) time intervals.

For example, you can specify scheduling sessions as follows: 12:00–14:00 and 18:00–8:00 from Monday to Friday; 8:00–12:00 and 17:00–8:00 from Saturday to Sunday.

Overview

Feature	Description
Configuring a Scheduling Session	Specifies a scheduling session.
Scheduling AP Radio	Applies the scheduling session to an RF connector of an AP to enable or disable an AP radio at a scheduled time.
Scheduling WLAN	Applies a scheduling session to a WLAN to enable or disable the WLAN at a scheduled time.

1.3.1 Configuring a Scheduling Session

Specify a scheduling session.

Working Principle

Before using the scheduling function, a scheduling session needs to be created first to specify the time for RF scheduling. Then the scheduling session can be applied to an AP RF connector or WLAN.

Configuring a Scheduling Session

First, you need to create a scheduling session and specify the time and cycle.

For example, in the preceding example, if you want to provide wireless access services only in the daytime to teaching building, you can first create a scheduling session to specify the cycle as every day, and the scheduling interval as a period at night, for example, 21:00 to 6:00. If you want to provide WLAN services to customers of a bank only in the business hours of workdays, you can create a scheduling session to specify the cycle as workdays, and the scheduling time interval as off hours, for example, 18:00 to 9:00; and you can create the other cycle as weekends, and the scheduling interval as all day.

1.3.2 Scheduling AP Radio

Enable or disable the AP radio periodically.

Working Principle

Before using the scheduling function, a scheduling session needs to be created first to specify the time for RF scheduling. Then you can apply the scheduling session to an AP RF connector.

When the scheduling session starts or ends, the system sends a scheduling message. The processing logic of the scheduling message will enable or disable the RF connector of an AP or the RF connectors of an AP group where this scheduling session is applied.

↘ Applying a Scheduling Session on an RF connector

After a scheduling session is created, it must be applied to the corresponding AP RF connector so that the scheduling can take effect.

Three modes are available to apply a scheduling session.

Based on all APs

Based on AP groups

Based on a single AP

In these modes, a Radio ID can be specified or not. If no Radio ID is specified, the scheduling will take effect on all radios of the AP.

In the preceding example, you can specify the radios of the AP as required.

AP group-based configuration mode is most convenient if all APs in all buildings of the university are in the same AP group or in a few AP groups. If all APs in the university are deployed in the teaching buildings, the configuration mode based on all APs is also recommended. In the worst case, the configuration mode based on a single AP can be used to specify the Radio ID of the AP one by one.

↘ Handling of a Scheduling Message

After a scheduling session is created and the cycle and interval are specified, the system will start the timer of the scheduling session, and send a message after entering or exiting from this scheduling session. A scheduling message includes the following information:

- Scheduling Session ID
- Message type: the scheduling state, including entering and exiting from the scheduling session

The handling of a scheduling message covers all APs. The system will first check the session IDs configured on the AP, AP group, and all APs to determine whether the radio of the AP enters the scheduling state in descending order of priority.

Scheduling session ID priority in descending order: session ID configured on the AP, session ID configured on the AP group, and session ID configured on all APs. That is, if a scheduling session ID is configured on an AP, the session ID configured on its group or on all APs is invalid for the AP. If no session ID is configured on the AP, the session ID configured on its group takes effect for the AP. If no session ID is configured on the AP group to which the AP belongs, the session ID configured on all APs takes effect for the AP.

If the scheduling session ID in effect on the radio of the AP is the same as that in the scheduling message, the message type will be checked. If the scheduling state is entering the scheduling session, the radio of the AP will be disabled. Otherwise, the radio will be enabled.

1.3.3 Scheduling WLAN

Enable or disable a WLAN periodically.

Working Principle

Before using the scheduling function, a scheduling session needs to be created first to specify the time for WLAN scheduling. Then the scheduling session can be applied to a WLAN.

When the scheduling session starts or ends, the system sends a scheduling message. In the handling of the scheduling message, the processing logic will locate the WLAN where this scheduling session is applied to, and enable or disable the WLAN.

Applying a Scheduling Session on an RF connector

After the scheduling session is created, it must be applied to the corresponding WLAN so that the scheduling can take effect.

You need to specify in WLAN configuration mode the scheduling Session ID for the WLAN.

Handling of a Scheduling Message

After a scheduling session is created and the cycle and interval are specified, the system will start the timer of the scheduling session, and send a message after entering or exiting from this scheduling session. A scheduling message includes the following information:

- Scheduling Session ID
- Message type: entering or exiting from the scheduling session

The handling of a scheduling message covers all WLANs. The system will first check the session to which the WLAN is applied. If the scheduling Session ID to which the WLAN is applied is the same as that in the message, the message type will be checked. If in the scheduling state, the WLAN will be disabled. Otherwise, the radio will be enabled.

1.4 Configuration

Configuration	Description and Command	
Configuring AP Radio Scheduling	⚠ (Mandatory) It is used to create a scheduling session, specify the time interval, and apply the scheduling session to an AP or AP group.	
	schedule session	Creates a scheduling session.
	schedule session time-range	Specifies the time interval of a scheduling session.
	schedule session	Applies the scheduling session to an AP or an AP group.
Configuring WLAN Scheduling	⚠ (Mandatory) It is used to create a scheduling session and apply it to a WLAN.	
	schedule session	Creates a scheduling session.

	schedule session time-range	Specifies the time interval of a scheduling session.
	schedule session	Applies the scheduling session to a WLAN.

1.4.1 Configuring AP Radio Scheduling

Configuration Effect

- Create a scheduling session, specify a scheduling interval, and applies this scheduling session to an AP or an AP group to realize AP RF scheduling.

Configuration Steps

↘ Creating a Scheduling Session

- (Mandatory) In global configuration mode, run the **schedule session** *session-id* command to create a scheduling session. *session-id* indicates Session ID, which can be set to a value ranging from 1 to 8 on a fat AP.
- A scheduling session must first be created before use.
- Create a scheduling session on an AP where the scheduling function needs to be enabled.

Command	**schedule session** *session-id*
Parameter Description	*session-id*: Indicates Session ID. It can be set to a value ranging from 1 to 8 on a fat AP.
Defaults	By default, no scheduling session is created.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Specifying the Time Interval for a Scheduling Session

- (Mandatory) Run **schedule session** *session-id* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2* to specify the time interval and cycle of a scheduling session.
- Specify the time interval for a scheduling session on an AP where the scheduling function needs to be enabled.

Command	**schedule session** *session-id* **time-range** *n* **period** { *day1* [**to** *day2*] | **everyday** } **time** { *hh1:mm1* **to** *hh2:mm2* | **all-day** }
Parameter Description	*session-id*: Indicates Session ID. It can be set to a value ranging from 1 to 8 on a fat AP. *n*: Indicates the number of a time interval, which ranges from 1 to 8. *day1*: Indicates the start date of the scheduling session cycle, which can be set to { Mon, Tue, Wed, Thu, Fri, Sat, Sun }. **to** *day2*: *day2* indicates the end date of the scheduling session cycle. By default, this parameter indicates that the scheduling cycle is one day.

	everyday: Indicates that the session occurs every day, which is the simplified form of **period** *sun* **to** *sat*. **time** *hh1:mm1* **to** *hh2:mm2*: Indicates the scheduling time period, and *hh1:mm1* and *hh2:mm2* indicate the start time and end time respectively in the unit of hours (ranging from 0 to 23) and minutes (ranging from 0 to 59). **time all-day**: Indicates that the session time range is a whole day, which is the simplified form of **time** *00:00* **to** *23:59*.
Defaults	No time period or cycle is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Applying a Scheduling Session

- Mandatory.
- In AP configuration mode, run the **schedule session** *sid* command to specify the Session ID for APs or a single AP
- Apply a scheduling session on an AP where the scheduling function needs to be enabled.
- After a scheduling session is applied, if there is a scheduling message about the session, the RF connector on the AP is automatically managed and enters or exits from the scheduling session based on the type of the scheduling message.

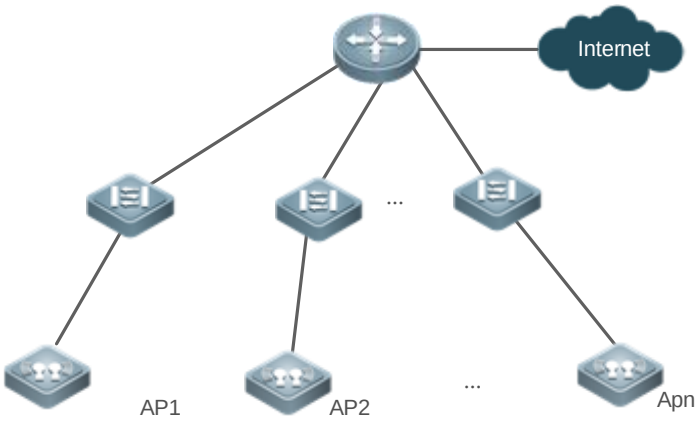
Command	**schedule session** *session-id*
Parameter Description	*session-id*: Indicates Session ID. It can be set to a value ranging from 1 to 8 on a fat AP.
Defaults	No scheduling session is applied.
Command Mode	Dot11radio interface configuration mode.
Usage Guide	N/A

Verification

- Run **show running-config** to display configurations on RF scheduling.
- Check whether scheduling is still performed for AP RF after a scheduling session expires.

Configuration Example

Providing Wireless Access Services During School Hours Only

Network Environment Figure 1-3	 A university adopts the fat AP architecture for its WLAN networking.
Steps	● Create a scheduling session. ● Set the scheduling time period for a scheduling session to the evening. Hostname# configure terminal Hostname(config)# schedule session 1 Hostname(config)# schedule session 1 time-range 1 period sun to sat time 21:00 to 6:00
Verification	● Run the **show running-config** command to check the scheduling configuration. ● Check the state of the AP radio within the scheduling time period. ● Check the state of the AP radio when the scheduling is not performed. Hostname# show running-config ..... schedule session 1 schedule session 1 time-range 1 period Sun to Sat time 21:00 to 06:00 ..... interface Dot11radio 1/0 schedule session 1 .....

Common Errors

- No scheduling session is created.
- The interval of the scheduling session is not properly configured.
- The scheduling priorities on the AP are in conflict.
- Scheduling is not applied to the target radio.

1.4.2 Configuring WLAN Scheduling

Configuration Effect

- Create a scheduling session, specify a scheduling interval, and apply this scheduling session to a WLAN to realize WLAN scheduling.

Configuration Steps

↘ Creating a Scheduling Session

- (Mandatory) In WLAN configuration mode, run the **schedule session** *session-id* command to specify the scheduling Session ID of a WLAN.
- After a scheduling session is applied, if the message for the scheduling session is displayed, the specified WLAN interface will automatically enter or exit from the scheduling state as specified by the massage type.
- Create a scheduling session on an AP where the scheduling function needs to be enabled.

Command	**schedule session** *session-id*
Parameter Description	**session** *session-id*: Indicates Session ID. It can be set to a value ranging from 1 to 8 on a fat AP.
Defaults	No scheduling session is applied on a WLAN.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Specifying the Time Interval for a Scheduling Session

- Mandatory.
- Specify the time interval for a scheduling session on an AP where the scheduling function needs to be enabled.

Command	**schedule session** *session-id* **time-range** *n* **period** { *day1* [**to** *day2*] | **everyday** } **time** { *hh1:mm1* **to** *hh2:mm2* | **all-day** }
Parameter Description	*session-id*: Indicates Session ID. It can be set to a value ranging from 1 to 8 on a fat AP. *n*: Indicates the number of a time interval, which ranges from 1 to 8. *day1*: Indicates the start date of the scheduling session cycle, which can be set to { Mon, Tue, Wed, Thu, Fri, Sat, Sun }. **to** *day2*: *day2* indicates the end date of the scheduling session cycle. By default, this parameter indicates that the scheduling cycle is one day. **everyday**: Indicates that the session occurs every day, which is the simplified form of **period** *sun* **to** *sat*. **time** *hh1:mm1* **to** *hh2:mm2*: Indicates the scheduling time period, and *hh1:mm1* and *hh2:mm2* indicate the start time and end time respectively in the unit of hours (ranging from 0 to 23) and minutes (ranging from 0 to 59). **time all-day**: Indicates that the session time range is a whole day, which is the simplified form of **time** *00:00* **to** *23:59*.

Defaults	By default, a scheduling session is not configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Applying a Scheduling Session

- Mandatory.
- Apply a scheduling session on an AP where the scheduling function needs to be enabled.

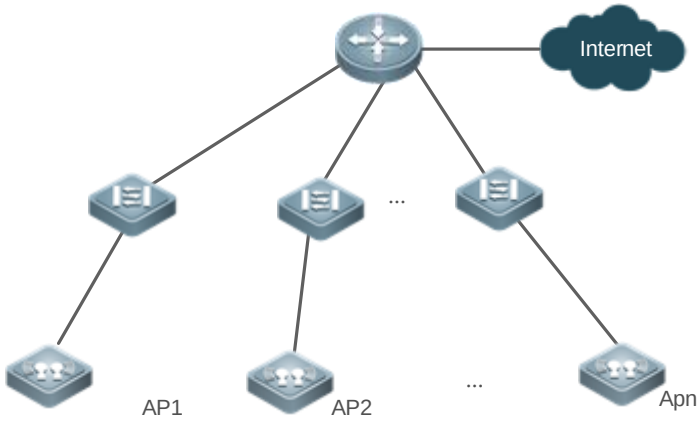
Command	**schedule session** *session-id*
Parameter Description	*session-id*: Indicates Session ID. It can be set to a value ranging from 1 to 8 on a fat AP.
Defaults	No scheduling session is applied on a WLAN.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run **show running-config** to display configurations on RF scheduling.
- Check whether scheduling is still performed for a WLAN after a scheduling session expires.

Configuration Example

Enabling the WLAN for Bank Customers Only During Working Hours on Workdays

Network Environment Figure 1-4	 A bank adopts the fat AP architecture for its WLAN networking. WLAN 99 with the SSID **wlan bank-free** is available for customers. AP1, AP2, ..., and APn are deployed in the business hall of the bank.

Steps	● Create a scheduling session. ● Set the scheduling time period for a scheduling session to the weeknights and all days on weekends. ● Apply the scheduling session to WLAN 99. Hostname# configure terminal Hostname(config)# schedule session 1 Hostname(config)# schedule session 1 time-range 1 period mon to fri time 18:00 to 9:00 Hostname(config)# schedule session 1 time-range 2 period sat to sun time 00:00 to 23:59 Hostname(config)# dot11 wlan 99 Hostname(dot11-wlan-config)# schedule session 1
Verification	● Run the **show running-config** command to check the scheduling configuration. ● Check the state of the AP radio within the scheduling time period. ● Check the state of the AP radio when the scheduling is not performed. Hostname# show running-config …… schedule session 1 schedule session 1 time-range 1 period mon to fri time 18:00 to 9:00 schedule session 1 time-range 2 period sat to sun time 00:00 to 23:59 …… dot11 wlan 99 schedule session 1 ……

Common Errors

- No scheduling session is created.
- The interval of the scheduling session is not properly configured.

1.5 Monitoring

Displaying

Description	Command
Display configuration about scheduling sessions	**show schedule session** [*session-id*]

1 Configuring Wireless Location

1.1 Overview

The Wireless Location (WL) function uses 802.11 wireless signals to locate terminal stations (STAs). It is supported on all 802.11 a/b/g/n-compliant STAs, such as laptops, Mobile Units (MUs), and special Radio Frequency Identifications (RFIDs, hereinafter mainly referred to as TAGs). By analyzing and summarizing 802.11 wireless signals sent from these STAs, WL achieves STA locations through software on the location server in vivid forms such as maps, tables, or reports.

The WL function also has the following characteristics:

- Support indoor and outdoor deployment.
- Support two algorithms, Received Signal Strength Indication (RSSI) location and Time Difference of Arrival (TDOA) location.
- Support two RFIDs, MUs and TAGs.

1.2 Applications

Application	Description
Centralized Location Deployment	Deploys the location system in fit AP mode.

1.2.1 Centralized Location Deployment

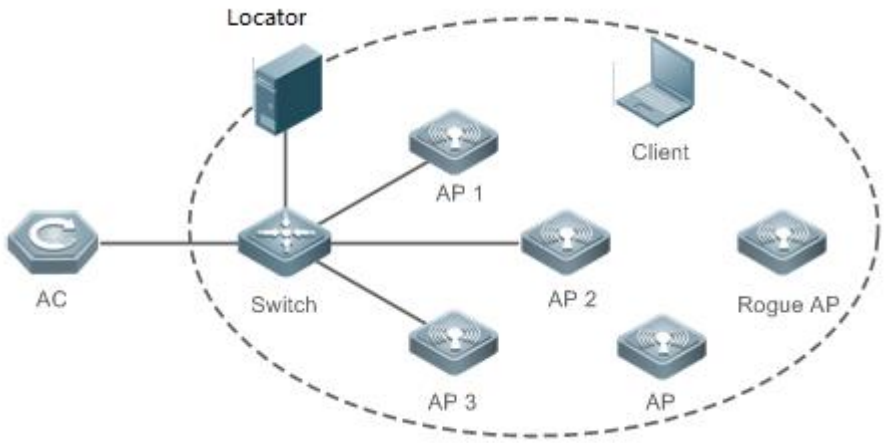
Scenario

Under WLAN in fit AP mode where Access Points (APs) are managed uniformly by the Access Controller (AC), the 802.11 STAs can be located by a Location Server or Locator. The special requirements are:

- Direct access is required between APs and the Locator. Therefore, make sure the ping between them is successful.
- The APs must be WL-capable Ruijie products.
- It is necessary to deploy three APs for accurate location.

The following figure is an example where AP 1, AP 2 and AP 3 can communicate with the Locator. Three APs respectively send received STA information to the Locator which then works out the STA locations.

Figure 1-1



Deployment

- The AC is responsible for WL configuration management and issuing.
- The APs are responsible for collecting STA information and sending the information as specified to the Locator.
- The Locator summarizes all the information sent from all APs, works out the STA locations, and displays the locations in maps or tables based on configurations by the administrator.

1.3 Features

Basic Concepts

A location system contains three parts: the Target or Source, the Receiver, and the Backend Location System.

↘ Target or Source

WL supports two types of location targets:

- TAGs, produced by AeroScout, a type of light and portable RFIDs which are usually placed or stuck on the targets to be located.
- MUs, 802.11-complicant wireless STAs regularly transmitting wireless signals.

↘ Receiver

The Receiver can be a Ruijie AP or an AeroScout Tag exciter (used not to collect locations but to excite the TAGs to transmit specified wireless signals).

↘ Backend Location System

The Backend Location System includes a Locator, AeroScout Engine (AE) computing software and all kinds of graphic programs.

Features

Feature	Description

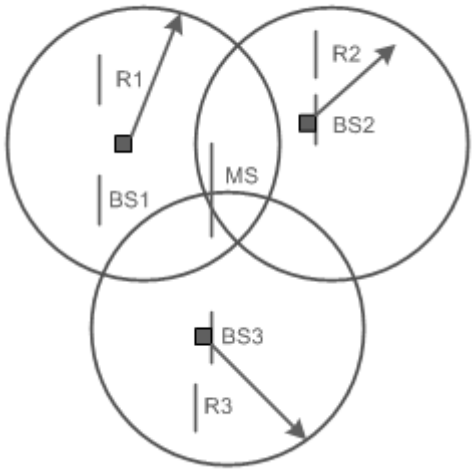
WL	Enables WL for APs.

1.3.1 WL

Working Principle

Based on the measurement of RSSI from an MU received by a base station (BS) and the channel transmission model, the distance between them can be estimated to be d. In this way, for a BS (i), the MU must be on the circle centered at BS (i) with a radius of d. When three or more BSs are used for distance measurement of the same MU, the location of this MU can be determined. In this method, the main causes for location error are the multipath effect generated during signal transmission and the shadow effect generated during obstacle crossing. More accurate location can be achieved in open space without obstacles. However, in many circumstances, the location accuracy is significantly affected because of uncertainties, such as the multipath effect, attenuation, and scattering, due to various obstacles.

Figure 1-2



1.4 Configuration

Configuration	Description and Command	
Configuring WL Basic Features	⚠ (Mandatory) It is used to enable WL.	
	wlocation enable	Enables WL on a specified AP.
	wlocation ae-ip	Configures the IP address of the Locator connected to a specified AP.
	wlocation ae-port	Configures the port ID (PID) of the Locator connected to a specified AP.
	wlocation mu enable	Enables MU location on a specified AP.
	wlocation tag enable	Enables TAG location on a specified AP.

Configuration	Description and Command	
	(Optional) It is used to optimize the WL transmission.	
	wlocation compound enable	Enables the WL aggregation.
	wlocation send-mu-time	Configures the interval for sending MU location information on a specified AP.
	wlocation send-tag-time	Configures the interval for sending TAG location information on a specified AP.
	wlocation mu report enable	Enables WL location report.
	wlocation tag report enable	Enables TAG location report.
	wlocation mu report reduce enable	Simplifies MU location information.
	wlocation ignore beacon enable	Filters Beacon packets sent by APs.

1.4.1 Configuring WL Basic Features

Configuration Effect

- Enable WL to provide basic location services.

Notes

- N/A

Configuration Steps

↘ Enabling WL on an AP

- Mandatory.
- Run the **wlocation enable** command to enable WL on an AP.
- Specify WL targets by running the **wlocation mu enable** and **wlocation tag enable** commands, which are used to enable WL for MUs and TAGs respectively.
- If WL is not enabled or no WL target is specified, WL cannot be used.
- Except as otherwise noted, enable WL for each AP in the deployment where location is required.

Command	**wlocation enable** [**radio** *radio-id*]
Parameter Description	*radio-id*: Enables or disables the radio.
Defaults	WL is disabled.
Command Mode	Wlocation configuration mode
Usage Guide	N/A

↘ Configuring the IP Address and PID for the Locator

- Mandatory.

- The PID is defaulted depending on the configuration of a specific Locator.
- The WL of APs works only with the Locator. Therefore, the IP address and PID of the Locator needs to be configured, guaranteeing its communication with the APs.
- The commands for configuring the IP address and PID are **wlocation ae-ip** *ip-address* and **wlocation ae-port** *port* respectively.

Command	**wlocation ae-ip** *ip-address*
Parameter Description	*ip-address*: IP address of the Locator
Defaults	No IP address is configured for the Locator. The AE server's default IP address is 0.0.0.0.
Command Mode	Wlocation configuration mode
Usage Guide	N/A

Command	**wlocation ae-port** *port*
Parameter Description	*port*: PID of the Locator, in the range from 1024 to 65535.
Defaults	The default PID is 12092.
Command Mode	Wlocation configuration mode
Usage Guide	N/A

Enabling MU or TAG Location

- Mandatory.
- To enable WL on an AP, you need to enable WL for MUs or TAGs. The configuration depends on the scenario and the STA to be located.

Command	**wlocation mu enable**
Parameter Description	N/A
Defaults	MU location is disabled.
Command Mode	Wlocation configuration mode
Usage Guide	Both MU and TAG locations can be enabled at the same time.

Command	**wlocation tag enable**
Parameter Description	N/A
Defaults	TAG location is disabled.
Command Mode	Wlocation configuration mode
Usage Guide	Both MU and TAG locations can be enabled at the same time.

Configuring the Interval for Sending MU or TAG Location Information

- Optional.
- It is used to adjust the interval for sending location information. Except as otherwise noted, the default value is applicable.
- In the scenarios with a lot of STAs to be located, reduce the interval to avoid information losses. (An AP can cache 500 to 700 pieces of location information.)

Command	**wlocation compound enable**
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Wlocation configuration mode
Usage Guide	N/A

Command	**wlocation send-mu-time** *interval*
Parameter Description	*interval*: time interval, ranging from 100 to 600,000 ms
Defaults	The default interval is 300 ms.
Command Mode	Wlocation configuration mode
Usage Guide	N/A

Command	**wlocation send-tag-time** *interval*
Parameter Description	*interval*: time interval, ranging from 100 to 5,000 ms
Defaults	The default interval is 300 ms.
Command Mode	Wlocation configuration mode
Usage Guide	N/A

Enabling MU Location Report

- Optional.
- The Locator does not intercommunicate with APs which directly send collected MU location information, for example, through the NAT network. Except as otherwise noted, the default value is applicable.

Command	**wlocation mu report enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Wlocation configuration mode
Usage Guide	With this function enabled, the handshake process of the protocol (referring to the private

	protocol provided by Aeroscout itself for intercommunication between the Locator and APs) is ignored except through the NAT.

Enabling TAG Location Report

- Optional.
- The Locator does not intercommunicate with APs which directly send collected TAG location information, for example, through the NAT network. Except as otherwise noted, the default value is applicable.

Command	**wlocation tag report enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Wlocation configuration mode
Usage Guide	With this function enabled, the handshake process of the protocol (referring to the private protocol provided by Aeroscout itself for intercommunication between the Locator and APs) is ignored except through the NAT.

Simplifying MU Location Information

- Optional.
- Use this command where there is a requirement for lower traffic bandwidth, and the deployed location system interconnects with the location server developed by Ruijie Networks. Except as otherwise noted, you can apply the configuration on your demand.

Command	**wlocation mu report reduce enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Wlocation configuration mode
Usage Guide	Enable the function of simplifying MU location information to reduce bandwidth traffic, which applies only when the deployed location server is developed by Ruijie Networks.

Filtering Beacon Packets Sent by APs

- Optional.
- Use this command where there is a requirement for traffic bandwidth reduction. Except as otherwise noted, you can apply the configuration on your demand.

Command	**wlocation ignore beacon enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Wlocation configuration mode
Usage Guide	Enable the function of filtering Beacon packets sent by APs in Wi-Fi environment to reduce

	bandwidth traffic.

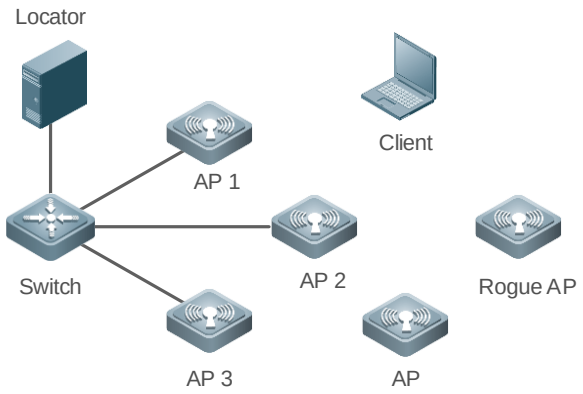
Verification

In the deployed network, enable STAs to send wireless packets.

- Verify that APs receive wireless location information.
- Verify that the Locator receives location information.

Configuration Example

↘ Enabling WL

Scenario Figure 1-3	
Configuration Steps	● Enable WL. ● Configure the IP address of the Locator. ● Enable MU location as required. ● Enable TAG location as required. ● Assuming that AP1 in the above figure is named ap1-1, run the following commands to enable ML for this AP.
AP1	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# wlocation Hostname(config-wlocation)# wlocation enable Hostname(config-wlocation)# wlocation ae-ip 1.1.1.1 Hostname(config-wlocation)# wlocation mu enable Hostname(config-wlocation)# wlocation tag enable
Verification	● Run the **show running** command to display the configurations of each AP and verify ML configuration. ● Assuming that AP1 in the above figure is named ap1-1, run the following commands to verify

	the ML configuration for this AP.
AP1	Hostname# show running config-wlocation ap1-1 wlocation enable wlocation ae-ip 1.1.1.1 wlocation mu enable wlocation tag enable

Common Errors

N/A

Configuring Wireless Security

1. Configuring RSNA
2. Configuring STA Access Control Lists
3. Configuring WIDS

1 Configuring RSNA

1.1 Overview

The Robust Security Network Architecture (RSNA) function provides security mechanisms for WLANs.

A WLAN uses open media and public electromagnetic waves as a carrier to transmit data signals. Neither communication party is connected with a cable. If transmission links are not properly protected through encryption, data transmission will be at great risk. Therefore, security mechanisms are especially important in a WLAN.

To enhance the security, a WLAN should be provided with at least the authentication and encryption mechanisms:

- Authentication mechanism: The authentication mechanism is used to authenticate users and allow only specified users (authorized users) to use network resources.
- Encryption mechanism: The encryption mechanism is used to encrypt data on wireless links to ensure that WLAN data can be received and understood only by expected users.

Protocols and Standards

- IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements -2007
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard -Aug 2004
- Information technology – Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements – 802.11, 1999 IEEE Standard for Local and metropolitan area networks "Port-Based Network Access Control" 802.1X™ -2004
- 802.11i IEEE Standard for Information technology –Telecommunications and information exchange between systems –Local and metropolitan area networks – Specific requirements

1.2 Applications

Application	Description
WEP Encryption	In a small WLAN that has a lower requirement for security; static WEP encryption can be used to protect wireless data communication.
PSK Access Authentication	For small and medium-sized enterprise networks or family users, access authentication based on pre-shared keys can be used to enhance the security of WLANs.
802.1X Access Authentication	For a scenario that has a higher requirement for security or unified management, port-based network access control can be used.

1.2.1 WEP Encryption

Scenario

In a small WLAN that has a lower requirement for security, WEP encryption can be used.

WEP encryption can use the open-system or shared-key link authentication mode. Their differences are as follows:

- When open-system link authentication is used, WEP keys can be used only for data encryption. Even if inconsistent keys are configured, users can go online; however, data transmitted after the users go online is discarded by the receiver due to key inconsistency.
- When shared-key link authentication is used, WEP keys are used for link authentication and data encryption. If inconsistent keys are configured, link authentication fails and the client cannot go online.

Deployment

- Configure WLAN on APs.
- Configure WEP encryption on APs in WLAN security configuration mode.

1.2.2 PSK Access Authentication

Scenario

Small and medium-sized enterprise networks or family users can use the WPA or WPA2 standard to enhance WLAN security. The simplest method is to use the pre-shared key authentication (referred to as WPA-PSK and WPA2-PSK respectively). In this case, WPA is similar to WEP, but users can achieve higher security through WPA and 802.11i, including more robust authentication and better encryption algorithms.

In PSK authentication, the same pre-shared key should be configured for a STA and an AP to establish connection and communication. No additional authentication server is required.

Deployment

- Configure WLAN on APs.
- Configure PSK authentication on APs in WLAN security configuration mode.
- Use this authentication with Web authentication to support Web authentication and charging.

1.2.3 802.1X Access Authentication

Scenario

In a scenario that has a higher requirement for security, 802.1X authentication can be used.

802.1X is a port-based network access control protocol. This authentication mode is used to authenticate and control STAs at the port level. STAs connected to the ports can access a WLAN if they pass the authentication; otherwise, the STAs fail to access the WLAN.

Authentication client software needs to be installed on terminals to perform 802.1X authentication. However, in some cases, some devices cannot be installed with the software, for example, wireless printers. For the sake of network management and security, although these terminals have no 802.1X authentication client software, administrators need to control the access of these terminals. MAC Authentication Bypass (MAB) provides a solution for this application.

After the MAB function is deployed for a WLAN, a wireless device can automatically probe the MAC address of a connected terminal and uses the MAC address to initiate a request to the authentication server.

Deployment

- Configure WLAN on AP1 and AP2.
- Configure authentication server on AP1 and AP2.
- Configure 802.1X authentication on AP1 and AP2 in WLAN security configuration mode.

1.3 Features

Basic Concepts

WPA

Wi-Fi Protected Access (WPA) is a wireless security draft defined by the Wi-Fi Alliance. The IEEE802.11i standard is compatible with this draft.

RSN

The IEEE802.11i standard defines the concept of Robust Security Network (RSN): and makes many improvements against various defects of the WEP encryption mechanism. The functions are equal to WPA2 launched by the Wi-Fi Alliance.

TKIP

The Temporal Key Integrity Protocol (TKIP) is an enhancement on WEP security. TKIP provides key mixing, message integrity check and key mechanism re-generation for each packet, thus eliminating hidden risks of WEP.

AES

Advanced Encryption Standard (AES) is a new encryption standard published by the National Institute of Standards and Technology (NIST) of the United States. On October 2, 2000, the Rijndael algorithm designed by Joan Daemen and Vincent Rijmen from Belgium won with its excellent performance and anti-attack capabilities, and became the new-generation encryption standard AES.

CCMP

Counter CBC-MAC Protocol (CCMP) uses AES, which is safer than TKIP.

AKM

Authentication and Key Management (AKM) is an access authentication mode for users to access a WLAN.

SAE

Simultaneous Authentication of Equals (SAE) is a peer authentication interaction. There are three encryption policies available:

- HnP: Hunting-and-Pecking loop.
- H2E: Hash to Element.
- Both: Both Hunting-and-Pecking loop and Hash-to-Element are enabled. The device determines the encryption mode according to the client capability. If both modes are supported, H2E encryption is used preferentially.

OWE

Opportunistic Wireless Encryption (OWE) does not need users to enter authentication information, and STAs and APs negotiate temporary PMKs.

Overview

Feature	Description
Link Verification	Verify the security of a wireless link before a STA associates with a WLAN.
Access Authentication	Perform authentication for a STA that accesses a WLAN.
Wireless Data Encryption	Implement security protection for communication data of a STA that accesses a WLAN.
Management Frame Encryption	Implement encryption on management frames.
WPA3 Authentication	Perform authentication for a STA that accesses a WPA3 WLAN.

1.3.1 Link Verification

Link verification refers to 802.11 authentication, which is a low-level authentication mechanism. Link verification is performed when a STA associates with an AP over 802.11, which is earlier than access authentication. Before accessing a WLAN, the STA must be authenticated over 802.11. 802.11 authentication marks the beginning of the handshake process when a STA accesses a WLAN and the first step for network connection.

The IEEE 802.11 standard defines two approaches to link authentication:

- Open-system link authentication
- Shared-key link authentication

Working Principle

Open-System Link Authentication

Open-system link authentication allows all users to access a WLAN. In this sense, no data protection is provided, which means that no authentication is performed. In other words, if the authentication mode is set to open-system authentication, all STAs that request authentication can pass the authentication.

Open-system link authentication comprises two steps:

Step 1: A STA requests authentication. The STA sends an authentication request that contains the ID (usually the MAC address) of the STA.

Step 2: An AP returns the authentication result. The AP sends an authentication response that contains information indicating whether the authentication succeeds or fails. If the authentication succeeds, the STA and AP pass the bidirectional authentication.

Figure 1-1



↘ Shared-key Link Authentication

Shared-key link authentication is another authentication mechanism in addition to the open-system link authentication. Shared-key link authentication requires that the same shared key be configured for a STA and an AP. The shared-key link authentication can be configured only in static WEP encryption whereas the open-system link authentication is available in all the other modes.

The process of shared-key link authentication is as follows:

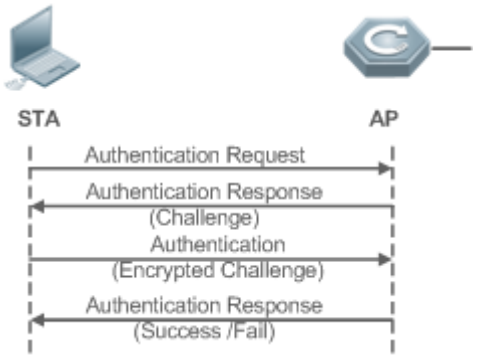
Step 1: A STA sends an authentication request to an AP.

Step 2: The AP generates a Challenge packet (a string) at random and sends the packet to the STA.

Step 3: The STA copies the received string to a new message, encrypts the message with a key and then sends the encrypted message to the AP.

Step 4: After receiving the message, the AP decrypts the message with the key, and then compares the decrypted string with the string sent to the STA. If the two strings are the same, it indicates that the STA has the same shared key as that on the AP and the shared-key authentication succeeds; otherwise, the shared-key authentication fails.

Figure 1-2



1.3.2 Access Authentication

Access authentication is a solution that enhances WLAN security.

After a STA is associated with an AP, whether the STA can use the service provided by the AP depends on the result of access authentication. If the STA passes the authentication, the AP enables the logical port for the STA; otherwise, the STA is not allowed to access the WLAN.

The IEEE 802.11 standard defines two access authentication approaches:

- PSK access authentication
- 802.1X access authentication

Working Principle

PSK Access Authentication

Pre-shared Key (PSK) is an 802.11i authentication mode, which performs authentication with pre-defined static keys. This authentication approach requires that a STA and an AP be configured with the same pre-shared key. If their keys are the same, the PSK access authentication succeeds; otherwise, the PSK access authentication fails.

802.1X Access Authentication

802.1X is a port-based network access control protocol. This authentication approach is used to authenticate and control the STAs at the port level. STAs connected to the ports can access resources in a WLAN if they pass the authentication; otherwise, the STAs cannot access resources in the WLAN.

A WLAN system with the 802.1X authentication function must provide the following elements to implement port-based authentication and authorization:

- Authentication client

Authentication client is generally installed on the STA. When the user wants to access the network, he activates the client program and enters the user name and password. Then, the client program sends a connection request.

- Authenticator

An authenticator means an AP or a communication device functioning as an AP. It is responsible for uploading and pushing user authentication information and enables or disables a port based on the authentication result.

- Authentication server

The authentication server checks whether a user has the right to use the services provided by the network system based on his identification information (user name and password), and enables or disables a port to the authentication system based on the authentication result.

MAB authentication uses a MAC address as the username to initiate a request to the authentication server. Therefore, it is not necessary for the terminal to install the client.

1.3.3 Wireless Data Encryption

Compared with a wired network, a wireless network is prone to greater security risks. Within an area, all WLAN devices share the same transmission medium and any device can receive data from all the other devices. This feature poses threat to WLAN data.

The IEEE 802.11i protocol defines the following encryption algorithms:

- WEP encryption
- TKIP encryption
- AES encryption

Working Principle

WEP Encryption

Wired Equivalent Privacy (WEP) is a data encryption mode specified in the original IEEE 802.11 standard, and is the basis for WLAN security authentication and encryption. WEP is used to promote the privacy of data exchanged between authorized users in a WLAN and prevent the data from being stolen.

WEP uses the RC4 algorithm to promote data privacy and implements authentication by using a shared key. WEP does not specify a key management scheme. Generally, keys are configured and maintained manually. WEP that does not provide a key distribution mechanism is called manual WEP or static WEP.

A WEP encrypted key may contain 64 bits or 128 bits. The 24-bit Initialization Vector (IV) is generated by the system. Therefore, a shared key to be configured on an AP and a STA consists of only 40 bits or 104 bits. In practice, the 104-bit WEP keys are widely used to replace the 40-bit WEP keys. WEP using 104-bit keys are called WEP-104. Although WEP-104 increases the security of WEP encryption, WEP encryption is prone to security risks due to limitations of the RC encryption algorithm and statically configured keys. WEP encryption cannot ensure the confidentiality and integrity of data or access authentication.

TKIP Encryption

Temporal Key Integrity Protocol (TKIP) is a temporary makeshift solution created by the IEEE 802.11 organization for fixing the WEP encryption mechanism. Like WEP encryption, TKIP encryption also uses the RC4 algorithm. But compared with WEP encryption, TKIP encryption can provide much safer protection for WLAN services in the following aspects:

A static WEP key is manually configured and all users within the same service area share the same key. A TKIP key is generated through dynamic negotiation, and each packet has a unique key.

– TKIP increases the key length from 40 bits to 128 bits, and the IV length from 24 bits to 48 bits, thus improving the security of WEP encryption.

– TKIP supports Message Integrity Check (MIC) and the replay prevention function.

AES Encryption

The Counter mode with CBC-MAC Protocol (AES-CCMP) is the most advanced wireless security protocol oriented to the public.

The IEEE 802.11i standard requires that CCMP be used to provide four security services, namely, authentication, confidentiality, integrity, and replay prevention. CCMP uses the 128-bit Advanced Encryption Standard (AES) to implement confidentiality and uses the CBC-MAC to ensure data integrity and authentication.

As a new advanced encryption standard, AES uses the symmetrical block encryption technology to provide better encryption performance than the RC4 algorithm in WEP/TKIP. It is the new-generation encryption technology that replaces WEP and brings more powerful security protection for WLANs.

1.3.4 Management Frame Encryption

Wireless management frames, such as authentication, de-authentication, association, disassociation, beacon, and probe frames, are transmitted using plaintext over the air interface. In this case, these frames may be used by illegal devices to attack wireless clients associated with APs. The Protected Management Frame (PMF) defined by the 802.11W protocol is a management frame subset, which includes frames of De-authentication, Disassociation, Spectrum Management, QoS, DLS, Block Ack, Radio measurement, SA Query, Protected Dual of Public Action, Fast BSS Transition, and Vendor-specific Protected. Packets in this subset will be encrypted when being transmitted over the air interface. The SA Query mechanism is used to prevent counterfeited association frames, de-authentication frames, and disassociation frames from disassociating STAs.

Working Principle

SA Query

When a STA is online and applies the PMF and an AP receives an association request from a counterfeited STA, the AP rejects the association request first and returns an association response with the status code 30, indicating that the association request is rejected temporarily and retry is required later. Then, the AP sends an SA Query request to the STA. If the STA is online, the STA sends an SA Query response. After the AP receives the SA Query response, it regards that the STA is online and does not process association requests within the association recovery time (10s). This prevents the real STA from being disassociated using counterfeited packets.

Similarly, when an online STA that applies the PMF receives an unencrypted disassociation or de-authentication frame, the STA sends an SA Query request to the AP. The AP returns an SA Query response. After the STA receives the SA Query response, it regards that the AP is still online and remains in the online state. This prevents the real STA from being disassociated using counterfeited packets.

1.3.5 WPA3 Authentication

Wi-Fi Protected Access 3 (WPA3) is a next-generation Wi-Fi encryption protocol released by the Wi-Fi Alliance. WPA3 is available in OWE, WPA3-Personal and WPA3-Enterprise editions. WPA3-Enterprise edition provides WPA3 Enterprise only and WPA3 Enterprise 192-bit modes.

- WPA3-Personal Edition

  WPA3-Personal uses Simultaneous Authentication of Equals (SAE) for management frame authentication to replace PSK authentication in WPA2-Personal. When a STA attempts to connect to the device enabled with WPA3-Personal, the SAE protocol used by WPA3 adds an SAE handshake before the original PSK 4-way handshake and introduces a dynamic random variable in the pairwise master key (PMK) generation process. The PMK negotiated each time is different, ensuring the randomness of the key. As such, SAE provides a more secure key authentication mechanism for WPA3 to address the security risks exposed by WPA2.

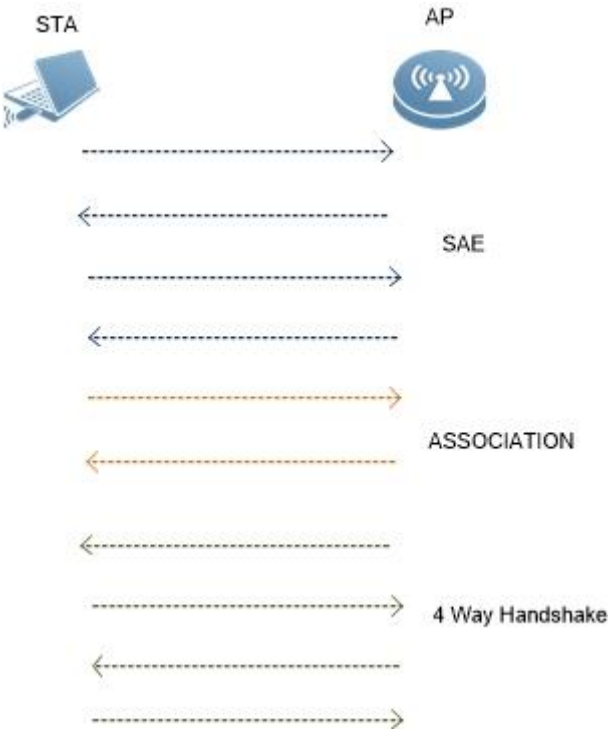
  There are three WPA3 SAE encryption options available:

  HnP: The algorithm relates the password with calculation time. It is theoretically possible to crack the password using time difference.

H2E: To address the shortcomings of HnP, the Wi-Fi Alliance introduced the Hash to Element (H2E) encryption algorithm in the third version of WPA3. In this method, the secret PWE used in the SAE protocol is generated from a password. H2E-incapable clients cannot authenticate using this encryption method.

Both: Both HnP and H2E are supported. If the client supports both encryption modes, H2E encryption is used preferentially. If not, HnP is used preferentially.

Figure 1-3 Mutual Authentication of WPA3-Personal Edition



- WPA3-Enterprise Edition

  Based on WPA2-Enterprise, the WPA3 Enterprise only mode introduces management frame protection. Deauthentication, Disassociation, Spectrum Management, QoS, DLS, Block Ack, Radio measurement, SA Query, Protected Dual of Public Action, Fast BSS, Transition, and Vendor-specific Protected packets are encrypted for transmission on the air interface to enhance security.

  Suite-B Cryptography (192 bits) suite is used for 4-way handshake in the WPA3 Enterprise 192-bit mode.

  1) Compared with the 128-bit key used by WPA2, this suite increases the key length to 192 bits, further improving the password defense strength and data security.
  2) 256-bit Galois/Counter Mode Protocol (GCMP-256) and 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) are used to protect multicast management frames.

- OWE Authentication

  Also known as enhanced open wireless authentication (Enhanced Open), it does not require users to input authentication information, but the packets exchanged between STAs and APs are still encrypted, providing a certain level of privacy and security against eavesdropping. In a scenario where OWE authentication is enabled, STAs that do not support OWE authentication are allowed to access in OPEN mode.

1.4 Configuration

Configuration	Description and Command	
Configuring Static WEP	⚠ (Mandatory) It is used to enable static WEP encryption.	
	wlansec	Enters the WLAN security configuration mode.
	security static-wep-key encryption	Enables static WEP for a WLAN and configures a static WEP key.
	⚠ (Optional) It is used to configure the link authentication mode.	
	security static-wep-key authentication	Configures the link authentication mode of static WEP.
Configuring WPA Authentication	⚠ (Mandatory) It is used to enable WPA authentication.	
	security wpa	Configures WPA authentication.
	security wpa ciphers	Configures the encryption mode of WPA authentication.
	security wpa akm	Configures the access authentication mode for WPA authentication.
	⚠ (Optional) It is used to configure a shared key for WPA PSK authentication.	
	security wpa akm psk set-key	Configures a shared key for WPA PSK authentication.
Configuring RSN Authentication	⚠ (Mandatory) It is used to enable RSN authentication.	
	security rsn	Configures RSN authentication.
	security rsn ciphers	Configures the encryption mode for RSN authentication.
	security rsn akm	Configures the access authentication mode for RSN authentication.
	⚠ (Optional) It is used to configure a shared key for RSN PSK authentication.	
	security rsn akm psk set-key	Configures a shared key for RSN PSK authentication.
Configuring MAB Authentication	⚠ (Optional) It is used to configure MAB authentication.	
	dot1x-mab	Enables MAB authentication.
Configuring Authentication Parameters	⚠ (Optional) It is used to configure key interaction parameters and the jitter prevention time in Web authentication.	
	authtimeout forbidcount	Configures the association forbidding count after four-way handshake key interaction fails.

Configuration	Description and Command	
	authtimeout forbidtime	Configures the association forbidding interval after four-way handshake key interaction fails.
	authtimeout groupcount	Configures the multicast key negotiation packet re-transmission count.
	authtimeout grouptime	Configures the timeout duration of multicast key negotiation packets.
	authtimeout paircount	Configures the uncast key negotiation packet re-transmission count.
	authtimeout pairtime	Configures the timeout duration of unicast key negotiation packets.
	webauth prevent-jitter	Configures the jitter prevention time of Web authentication.
Configuring Management Frame Encryption	⚠ (Optional) It is used to enable or disable management frame encryption.	
	security pmf { **disable** | **mandatory** | **optional** }	Enable or disable management frame encryption
Configuring WPA3 Authentication	**security wpa3 mode**	Sets the WPA3 authentication mode.
	security wpa3 personal passphrase	Sets a WPA3-Personal password.
Configures the Response Delay Mode for Authentication Packets	**rsna lazy-response enable**	Configures the response delay for authentication packets.
	rsna lazy-response time	Configures the response delay timeout for authentication packets.

1.4.1 Configuring Static WEP

Configuration Effect

- Enable static WEP encryption and provide WEP encryption protection for WLAN data.
- Configure the link authentication mode.

Notes

- The link authentication mode must be configured after static WEP encryption is enabled.
- In the security mode of a WLAN, static WEP encryption cannot be configured together with other authentication encryption.
- Only one WLAN can be configured with static WEP encryption

Configuration Steps

↘ Enabling Static WEP

- Mandatory.

- Enable static WEP encryption in WLAN security configuration mode on the AP.

Command	**security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*
Parameter Description	*key-length*: Specifies the key length, which can be 40 bits or 104 bits. **ascii**: Specifies that the WEP key is ASCII code. **hex**: Specifies that the WEP key is hexadecimal code. *key-index*: Specifies the key index, ranging from 1 to 4. *key*: Specifies key data.
Defaults	Static WEP is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to configure a static WEP key and enable static WEP. This command can be configured repeatedly, but only the last configuration takes effect. The key length must be the same as the *key-length* parameter in the command.

Configuring the Link Authentication Mode

- (Optional) The default link authentication mode is open-system link authentication. This command can be used to configure shared-key link authentication.
- The link authentication mode can be configured only after static WEP encryption is enabled. After configuring the sharedkey link authentication mode, set the link authentication mode to shared key link authentication on the STA; otherwise, the STA cannot access the WLAN.

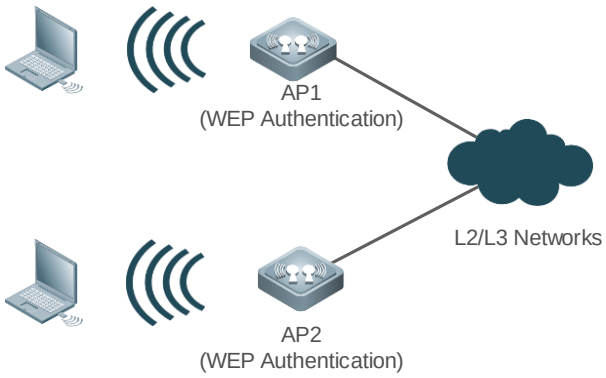
Command	**security static-wep-key authentication** { **open** | **share-key** }
Parameter Description	**open**: Configures open-system link authentication. **share-key**: Configures shared key link authentication.
Defaults	A STA accesses a WLAN by using open-system link authentication by default.
Command Mode	WLAN security configuration mode
Usage Guide	Configure the link authentication mode after configuring a static WEP key. The link authentication mode cannot be configured for other security configuration modes than static WEP.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring Static WEP Encryption and Using Shared-Key Link Authentication for WLAN 1

Scenario Figure 1-4	 In Fat AP mode, configure WLAN 1 on AP1 and AP2, and configure the security policies 1 as follows: 1. Enable static WEP encryption. 2. Configure shared-key link authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable static WEP encryption and configure a WEP key. ● Set the link authentication mode to shared-key link authentication.
AP	Hostname(config)#wlansec 1 Hostname(config-wlansec)# security static-wep-key encryption 40 ascii 1 12345 Hostname(config-wlansec)# security static-wep-key authentication share-key
Verification	Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.
AP	Hostname# show running-config | begin wlansec 1 wlansec 1 security static-wep-key encryption 40 ascii 1 12345 security static-wep-key authentication share-key !

Common Errors

- The configured key length is inconsistent with the specified key length.
- Static WEP is configured for multiple WLANs.
- The link authentication mode is configured before static WEP is enabled.

1.4.2 Configuring WPA Authentication

Configuration Effect

- Enable WPA authentication for a WLAN.
- Specify the access authentication mode and encryption mode in WPA authentication.

Notes

- When WPA authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, WPA authentication cannot be configured with WEP authentication.

Configuration Steps

Configuring WPA Authentication

- Mandatory.

Command	**security wpa** { **enable** | **disable** }
Parameter Description	**enable**: Enables WPA authentication. **disable**: Disables WPA authentication.
Defaults	WPA authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in WPA authentication only after WPA authentication is enabled; otherwise, the configuration does not take effect. When WPA authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode of WPA Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The encryption mode of WPA authentication can be configured only after WPA authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between a STA and the WLAN is protected by the corresponding encryption mode.

Command	**security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode of WPA authentication. **disable**: Disables the encryption mode of WPA authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode of WPA authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode of WPA authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. A STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security wpa akm** { **psk** | **802.1x** } { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode of WPA authentication. **disable**: Disables the access authentication mode of WPA authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for WPA Authentication

- (Optional) It must be configured when WPA PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AP.

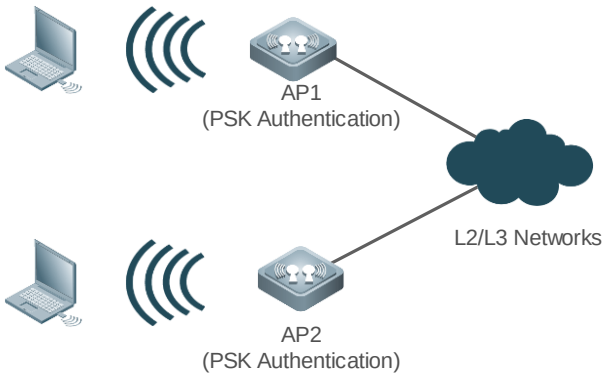
Command	**security wpa akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring WPA PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario Figure 1-5	 In Fat AP mode , configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure WPA PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable WPA authentication. ● Configure the AES encryption mode for WPA authentication. ● Configure the PSK access authentication mode for WPA authentication. ● Configure the PSK key 12345678.
AP	Hostname(config)# wlansec 1 Hostname(config-wlansec)# security wpa enable Hostname(config-wlansec)# security wpa ciphers aes enable Hostname(config-wlansec)# security wpa akm psk enable Hostname(config-wlansec)# security wpa akm psk set-key ascii 12345678
Verification	Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security wpa enable security wpa ciphers aes enable security wpa akm psk enable security wpa akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- A WPA encryption mode is configured before WPA authentication is enabled in WLAN security configuration mode.

- An access authentication mode is configured before WPA authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- A WPA PSK key is configured before WPA authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.3 Configuring RSN Authentication

Configuration Effect

- Enable RSN authentication for a WLAN.
- Specify the access authentication mode and encryption mode in RSN authentication.

Notes

- When RSN authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, RSN authentication cannot be configured with WEP authentication.

Configuration Steps

↘ Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AP.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

↘ Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.

- The encryption mode in RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between a STA and the WLAN is protected by the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode for RSN authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The access authentication mode in RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. A STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable | disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AP.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters.

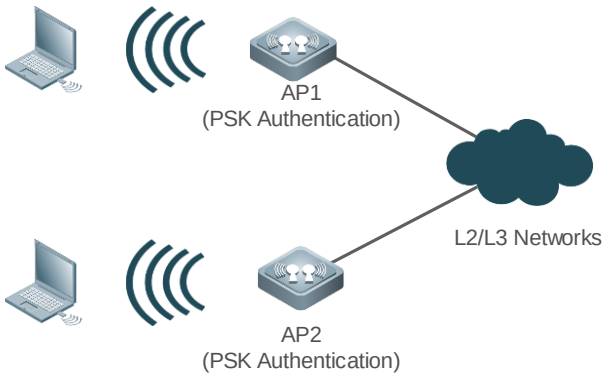
	hex: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring RSN PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario Figure 1-6	 In Fat AP mode, configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure RSN PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key to 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678.
AP	Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm psk enable Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678
Verification	Run the **show running-config**	**begin wlansec** command to check whether the configuration

	takes effect.
AP	Hostname# show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable security rsn akm psk enable security rsn akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- An RSN encryption mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- An access authentication mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- An RSN PSK key is configured before RSN authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.4 Configuring MAB Authentication

Configuration Effect

- Enable MAB authentication for a WLAN.

Notes

- In security mode of a WLAN, MAB authentication cannot be configured together with 802.1X access authentication or WEP authentication, but can be configured together with PSK authentication.

Configuration Steps

↘ Configuring MAB Authentication

- Mandatory.
- Enable MAB authentication in WLAN security configuration mode on the AP.
- Run the **dot1x-mab** command to enable MAB authentication or run the **no dot1x-mab** command to disable MAB authentication.

- MAB authentication can be configured independently, without RSN or WPA authentication enabled. MAB authentication can be used together with PSK access authentication, but cannot be used together with 802.1X access authentication.

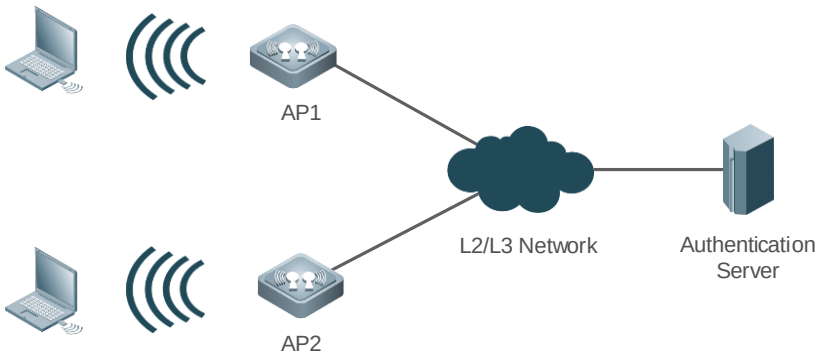
Command	dot1x-mab
Parameter Description	-
Defaults	MAB authentication is not configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable MAB authentication. MAB authentication can be used together with PSK access authentication, but cannot be used together with 802.1X access authentication.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring MAB Authentication for WLAN 1

Scenario Figure 1-7	 In Fat AP mode, configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure MAB authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable MAB authentication.
AP	Hostname# configure terminal Hostname(config)# aaa new-model Hostname(config)# radius-server host 192.168.32.120 Hostname(config)# radius-server key abcd@1234 Hostname(config)#wlansec 1 Hostname(config-wlansec)# dot1x-mab
Verification	Run the **show running-config**	**begin wlansec** command to check whether the configuration takes effect.
AP	Hostname#show running-config	begin wlansec 1 wlansec 1

	dot1x-mab !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- If 802.1X access authentication is enabled in WLAN security configuration mode, MAB authentication cannot be configured.

1.4.5 Configuring Authentication Parameters

Configuration Effect

- Configure key interaction parameters.
- Configure the jitter prevention time in Web authentication.

Notes

- Key interaction parameters take effect only in PSK or 802.1X authentication.
- The jitter prevention time in Web authentication can be configured only after Web authentication is enabled.

Configuration Steps

↘ Configuring Key Interaction Parameters

- Optional. Generally, it is unnecessary to configure key interaction parameters. It is recommended to set the packet re-transmission count and timeout duration to great values for a poor WLAN environment.
- It is configured in WLAN security configuration mode on the AP.

Command	**authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }
Parameter Description	**forbidcount** *count*: Configures the association forbidding count after four-way handshake key interaction fails. **forbidtime** *time*: Configures the association forbidding interval after four-way handshake key interaction fails. **groupcount** *count*: Configures the multicast key negotiation packet re-transmission count. **grouptime** *timeout*: Configures the timeout duration of multicast key negotiation packets. **paircount** *count*: Configures the unicast key negotiation packet re-transmission count. **pairtime** *timeout*: Configures the timeout duration of unicast key negotiation packets.
Defaults	The association is not forbidden after four-way handshake key interaction fails. The default multicast key negotiation packet re-transmission count is 4. The default timeout duration of multicast key negotiation packets is 1200 ms. The default unicast key negotiation packet re-transmission count is 4. The default timeout duration of unicast key negotiation packets is 1200 ms.

Command Mode	WLAN security configuration mode
Usage Guide	Key interaction parameters take effect only in PSK or 802.1X authentication.

Configuring the Jitter Prevention Time of Web Authentication

- Optional. The default jitter prevention time of Web authentication is 300 seconds. Users can configure the jitter prevention time based on actual requirements or disable the jitter prevention of Web authentication by setting the time to 0 seconds.
- It is configured in WLAN security configuration mode on the AP.

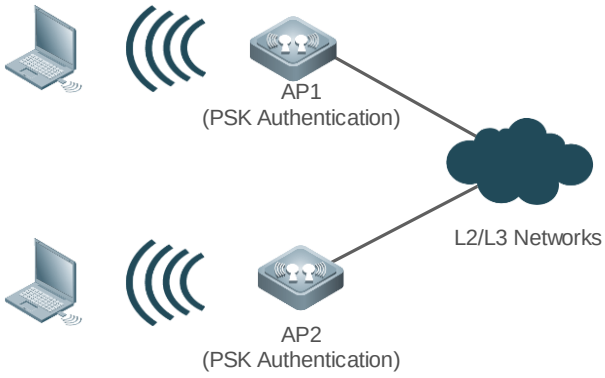
Command	**webauth prevent-jitter** *timeout*
Parameter Description	*timeout*: Configures the jitter prevention time of Web authentication, ranging from 0 to 86400 seconds (the jitter prevention of Web authentication is disabled when this parameter is set to 0).
Defaults	The default jitter prevention time of Web authentication is 300 seconds.
Command Mode	WLAN security configuration mode
Usage Guide	The jitter prevention time of Web authentication can be configured only after Web authentication is enabled.

Verification

Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.

Configuration Example

Configuring the RSN-PSK + Web Authentication Mode, the Unicast Key Negotiation Re-transmission Count to 5, and the Jitter Prevention Time of Web Authentication to 900 Seconds for WLAN 1

Scenario Figure 1-8	 In Fat AP mode, configure the security policies of WLAN 1 on AP1 and AP2 as follows: 1. Configure RSN PSK authentication. 2. Enable Web authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678.

	● Set the unicast key negotiation packet re-transmission count to 5. ● Configure Web authentication. ● Set the jitter prevention time of Web authentication to 900 seconds.
AP	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# aaa new-model Hostname(config)# radius-server host 192.168.197.79 key webkey Hostname(config)# aaa authentication web-auth default group radius Hostname(config)# aaa accounting network default start-stop group radius Hostname(config)# web-auth template eportalv2 Hostname(config.tmplt.eportalv2)# ip 192.168.197.79 Hostname(config.tmplt.eportalv2)# url http://192.168.197.79:8080/eportal/index.jsp Hostname(config.tmplt.eportalv2)# exit Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm psk enable Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678 Hostname(config-wlansec)# authtimeout paircount 5 Hostname(config-wlansec)# webauth Hostname(config-wlansec)# webauth prevent-jitter 900
Verification	Run the **show running-config** | **begin wlansec** command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable security rsn akm psk enable security rsn akm psk set-key ascii 12345678 webauth prevent-jitter 900 webauth authtimeout paircount 5

Common Errors

- The jitter prevention time of Web authentication is configured before Web authentication is enabled.

1.4.6 Configuring Management Frame Encryption

Configuration Effect

- Transmit partial management frames over the air interface in ciphertext format.

Notes

- Only WPA2 supports management frame encryption. If the WLAN uses Open, WEP-40, WEP-104 or WPA (AES or TKIP) for encryption, the management frame encryption function cannot be enabled.
- Not all STAs' OSs support management frame encryption.

Configuration Steps

Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AP.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured for RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The encryption mode for RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After a data encryption mode is configured for a WLAN and a STA accesses the WLAN, communication data of the STA is protected in the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable the AES or TKIP encryption mode for RSN authentication. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AP.
- The access authentication mode for RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.
  A STA can access a WLAN with access authentication enabled only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AP.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is an ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 characters. **hex**: Specifies that the PSK key is a hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	The shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Enabling Management Frame Encryption

- Mandatory.
- Enable management frame encryption on an AP.
- Management frame encryption can be configured only after RSN authentication is enabled.

Command	**security pmf** { **mandatory** | **optional** | **disable** }
Parameter Description	**mandatory**: The client needs to support management frame encryption. **optional**: The client does not need to support management frame encryption. **disable**: Disables management frame encryption.

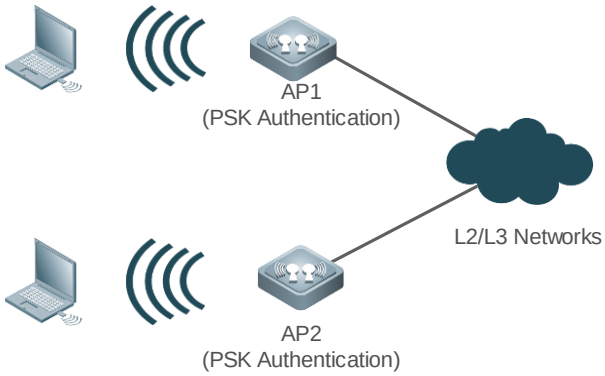
Defaults	Management frame encryption is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

Run the **show running-config | begin wlansec** command to check whether the configuration takes effect.

Configuration Example

↘ Enabling RSN-PSK Authentication and Management Frame Encryption for WLAN 1

Scenario Figure 1-9	 In Fat AP mode, configure the security policies of WLAN 1 on AP as follows: 1. Configure RSN PSK authentication. 2. Enable management frame encryption.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Set the data encryption mode for RSN authentication to AES. ● Set the access authentication mode for RSN authentication to PSK. ● Set the PSK key to 12345678. ● Enable management frame encryption.
AP	Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm psk enable Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678 Hostname(config-wlansec)# security pmf mandatory
Verification	Run the show running-config | begin wlansec command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable

	security rsn akm psk enable security rsn akm psk set-key ascii 12345678 security pmf mandatory

Common Errors

- WPA encryption is configured, but management frame encryption cannot be enabled.
- After **mandatory** is specified, a STA cannot go online because the STA does not support management frame encryption.

1.4.7 Configuring WPA3 Authentication

Configuration Effect

Enable the WPA3 authentication mode on a WLAN.

Notes

- WPA3-Personal can only work with WPA2 for authentication. WPA2 encrypts data on WLANs only using advanced encryption standard (AES).
- WPA3-Enterprise cannot be used with WPA2 simultaneously.
- WPA3 is subject to management frame encryption. Management frame encryption must be enabled before WPA3 can be enabled.
- In scenarios where WPA3-Enterprise authentication is adopted, STAs that do not support WPA3 cannot access a WLAN.

Configuration Steps

↘ Configuring Management Frame Encryption

- Mandatory.
- Perform the configuration in security configuration mode on a WLAN on the device.

Command	**security pmf** { **optional** | **mandatory** | **disable** }
Parameter Description	**mandatory**: Sets management frame encryption to mandatory mode. STAs must support management frame encryption. **optional**: Sets management frame encryption to optional mode. STAs do not need to support management frame encryption. **disable**: Disables management frame encryption.
Defaults	Management frame encryption is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	● When WPA3-Enterprise is used for authentication, management frame encryption must be set to mandatory mode. Otherwise, STAs may fail to access a WLAN. ● When WPA2 and WPA2 are used for authentication simultaneously, if management frame

	encryption is set to optional mode, STAs that support WPA2 and SAE are allowed to access a WLAN; if management frame encryption is set to mandatory mode, only WPA2 STAs that support Protected Management Frames (PMF) are allowed to access a WLAN.

Configuring the WPA3 Mode

- Mandatory.
- In WLAN security configuration mode, set the WPA3 mode.

Command	**security wpa3 mode** { **enhanced-open** | **enterprise** [**ccmp-128** | **gcmp-256**] | **none** | **personal** }
Parameter Description	**none**: Indicates that WPA3 is disabled. **enhanced-open**: Configures Opportunistic Wireless Encryption (OWE) authentication. **enterprise** : If the **ccmp-128** and **gcmp-256** parameters are not configured, GCMP-256 is used for authenticated encryption by default. **enterprise ccmp-128**: Configures CCMP-128 for WPA3-Enterprise authentication. **enterprise ccmp-256**: Configures GCMP-256 for WPA3-Enterprise authentication. **personal**: Configures WPA3-Personal authentication
Defaults	WPA3 is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	• WPA3-Personal can only work with WPA2 for authentication. WPA2 encrypts data on WLANs only using advanced encryption standard (AES). • WPA3-Enterprise cannot be used with WPA2 simultaneously. • WPA3 cannot be used with WPA simultaneously.

Configuring Equal-Cost WLANs for OWE Authentication

- (Optional) It must be used together with OWE authentication. After configuration, if the STA supports OWE authentication, it will access using OWE authentication. If the STA does not support OWE authentication, it will access in OPEN mode.

Command	**security wpa3 enhanced-open paired-wlan** { **none** | *wlan-id* }
Parameter Description	**none**: Clears the configuration of equivalent WLAN with OWE authentication. *wlan-id*: Configures the WLAN ID corresponding to the equivalent WLAN with OWE authentication.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	• The equivalent WLAN with OWE authentication must be pre-configured and set to OPEN. • QoS, Schedule, and other configurations of equivalent WLAN with OWE authentication must be consistent with those for OWE authentication. • After configuration, configure OWE authentication signals to hidden mode. An equivalent WLAN can only be associated with one OWE authentication signal.

Configuring a Password for the WPA3 Personal Mode

- The configuration is optional if WPA2 PSK authentication is enabled but mandatory when only the WPA3 Personal mode is enabled.
- STAs use the WPA2 PSK to access a WLAN in the WPA3-Personal/WPA2 mode.

Command	**security wpa3 personal passphrase** { **none** | **ascii** *word* }
Parameter Description	**none**: Clears the password. **ascii** *word*: Indicates a password in ASCII code, consisting of 8 to 63 characters.
Defaults	No password is configured for the WPA3 Personal mode by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuring WPA3 SAE Encryption Mode

- Mandatory.
- In WLAN security configuration mode, set the WPA3 SAE encryption mode.

Command	**security wpa3 personal pwe** { **hnp** | **h2e** | **both** }
Parameter Description	**hnp**: Configures HnP for WPA3 SAE authentication. **h2e**: Configures H2E for WPA3 SAE authentication. **both**: Configures both HnP and H2E for WPA3 SAE authentication. The device determines the encryption mode according to the client capability. If both modes are supported, H2E encryption is used preferentially.
Defaults	The default encryption mode is HnP.
Command Mode	WLAN security configuration mode
Usage Guide	• H2E encryption is more secure than HnP encryption. When both encryption modes are supported, H2E encryption is used preferentially. • If you configure H2E encryption, H2E-incapable clients will fail to access the network.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

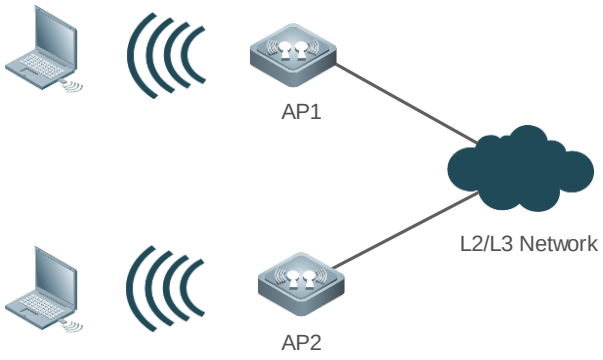
Configuration Example

Configuring the WPA3 Personal Authentication Mode for WLAN 1 with Password 12345678 and H2E Encryption Mode

Scenario	In a fat AP environment, configure the following security policies for WLAN 1: 1. Configure the pure WPA3 Personal authentication mode (RSNA disabled). 2. Set the shared key to 12345678. 3. Set the WPA3 SAE encryption mode to H2E.
Configuration	• Enter the security configuration mode of WLAN 1.

Steps	● Enable management frame encryption. ● Set the password to 12345678 for the WPA3 Personal mode. ● Set the WPA3 mode to Personal. ● Set the WPA3 SAE encryption mode to H2E.
AP	Hostname(config)#wlansec 1 Hostname(config-wlansec)#security pmf mandatory Hostname(config-wlansec)#security wpa3 personal passphrase ascii 12345678 Hostname(config-wlansec)#security wpa3 mode personal
Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AP	Hostname#show running-config | begin wlansec 1 wlansec 1 security pmf mandatory security wpa3 personal passphrase ascii 12345678 security wpa3 mode personal

Configuring the WPA3-Enterprise Authentication Mode for WLAN 1

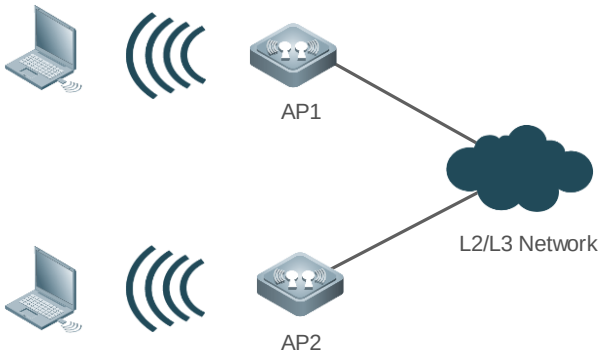
Scenario **Figure 1-10**	 In a fat AP environment, configure the following security policies for WLAN 1: 1. Configure management frame encryption. 2. Configure the WPA3-Enterprise authentication mode and set the encryption mode to the default.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Configure management frame encryption. ● Enable WPA3-Enterprise authentication mode and set the encryption mode to the default. Hostname(config)# aaa new-model Hostname(config)# aaa authentication dot1x default group radius Hostname(config)# aaa accounting network default start-stop group radius Hostname(config)# radius-server host 192.168.1.1 key daf13a124d Hostname(config)# dot1x accouting default Hostname(config)# dot1x authentication default Hostname(config)# wlansec 1 Hostname(config-wlansec)# security pmf mandatory Hostname(config-wlansec)# security wpa3 mode enterprise

Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check the configuration. Hostname#show running-config | begin wlansec 1 wlansec 1 security pmf mandatory security wpa3 mode enterprise

Configuring OWE Authentication for WLAN 1, and Configuring WLAN 2 as an Equivalent WLAN with OWE Authentication, Specifying WLAN ID as 2

Scenario

Figure 1-11



In a fat AP environment, configure the following security policies for WLAN on the AC:

1. Configure WLAN 1 to OWE authentication (ENHANCE-OPEN mode).
2. Set WLAN 2 to open.
3. Hide the SSID for WLAN 1.

Configuration Steps

- Add WLAN 1.
- Add WLAN 2.
- Enter the security configuration mode of WLAN 1.
- Enable management frame encryption.
- Configure OWE authentication. Configure WLAN 2 as an equivalent WLAN with OWE authentication.
- Enter the configuration mode of WLAN 1.
- Hide the SSID.

```
Hostname(config)#dot11 wlan 1
Hostname(config-wlan)#exit
Hostname(config)# dot11 wlan 2
Hostname(config-wlan)#exit
Hostname(config)#wlansec 1
Hostname(config-wlansec)#security pmf mandatory
Hostname(config-wlansec)#security wpa3 mode enhanced-open
Hostname(config-wlansec)#security wpa3 enhanced-open paired-wlan 2
Hostname(config-wlansec)#exit
Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)#no broadcast-ssid
Hostname(dot11-wlan-config)#exit
```

Verification	Run the **show running-config | begin wlansec** command to check whether the configuration takes effect.

AC	`Hostname#show running-config | begin wlansec 1`
	`wlansec 1`
	`security pmf mandatory`
	` security wpa3 enhanced-open paired-wlan 2`
	` security wpa3 mode enhanced-open`

Common Errors

- If you attempt to enable WPA authentication on a WLAN in WPA3 Personal mode, a configuration failure will be displayed.
- If you attempt to enable WPA2 (RSNA) authentication and set the cipher to TKIP in WPA3 Personal mode, a configuration failure will be displayed.

1.4.8 Configures the Response Delay Mode for Authentication Packets

Configuration Effect

To prevent STAs from being attacked by repeated authentication packets during the onboarding process, a response delay mode for authentication packets is added. After the response delay mode is enabled, the newly received authentication packets are discarded but previous authentication packets are still processed if association response packets are being processed within 1000 ms (by default). If the processing of association response packets has timed out (for example, association response packets are not processed properly within 1000 ms), previous association response packets are discarded and new authentication packets are processed.

Notes

N/A

Configuration Steps

↘ Configuring the Response Delay Mode

Command	**rsna lazy-response enable**
Parameter Description	This command has three forms: **rsna lazy-response enable:** Runs the command to enable the response delay mode. **no rsna lazy-response enable**: Runs the **no** form of the command to disable the response delay mode. **default rsna lazy-response enable**: Runs the **default** form of the command to restore the default configuration.
Defaults	The response delay mode is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Response Delay Timeout for Authentication Packets

Command	[**default**] **rsna lazy-response timer** *timer*
Parameter Description	*timer*: Configures the response delay timeout duration for authentication packets. The value is in milliseconds ranging from 0 to 2000. [**default**]: Restores the default configuration.
Defaults	1000
Command Mode	Global configuration mode
Usage Guide	N/A

1.5 Monitoring

Displaying

Description	Command
Displays security configuration of a WLAN.	**show wlan security** *wlan-id*
Displays security configuration of a STA.	**show wclient security** *mac-address*

1 Configuring STA Access Control Lists

1.1 Overview

STA access control lists indicate large-capacity static blacklists and whitelists and provide the following functions:

- Blacklist and whitelist for an access point (AP) or service set identifier (SSID).
- Blacklist and whitelist based on the organizationally unique identifier (OUI), matched based on the first three bytes of the vendor identifier in the media access control (MAC) address.
- The STA access control list configuration can be exported to a file or imported from a file.

Protocols and Standards

N/A

1.2 Applications

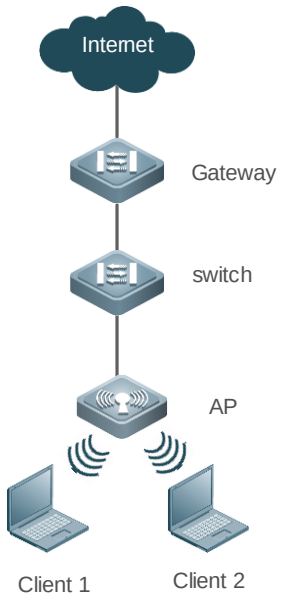
Application	Description
Fat AP Networking	Fat AP networking is adopted, including at least one AP and one STA.

1.2.1 Fat AP Networking

Scenario

On a wireless network, deploy a fat AP and enable the blacklist or whitelist of an AP or SSID, as shown in the Figure 1-1.

Figure 1-1



Remarks	PoE: switch, used as the gateway of the AP AP: wireless access point STA1 and STA2: wireless stations

Deployment

- Enable AP-based blacklist on the AP to add MAC addresses of illegal STAs to the blacklist.
- Enable SSID-based whitelist on the AP to allow STAs with specified MAC addresses to access this SSID only.

1.3 Features

Basic Concepts

N/A

Overview

Feature	Description
Configuring an AP-based Blacklist and Whitelist	Disallows STAs in the blacklist to access networks under the AP and allows STAs in the whitelist to access networks under the AP.
Configuring an SSID-based Blacklist and Whitelist	Disallows STAs in the blacklist to access the specific SSID and allows STAs in the whitelist to access the SSID.
Importing and Exporting Configurations	Exports configurations to a file or imports configurations from a file.

1.3.1 Configuring an AP-based Blacklist and Whitelist

You can add the MAC addresses of illegal STAs to the MAC address blacklist of the AP to prevent these STAs from accessing all networks under the AP.

If the network users are fixed, you can add the MAC addresses of legal STAs to the MAC address whitelist of the AP. In this case, only STAs with these MAC addresses can access networks under the AP.

To disallow or allow STAs of specific vendors to access the AP, add the OUIs of these STAs to the OUI blacklist or whitelist of the AP. In this case, STAs of these vendors are disallowed or allowed to access networks under the AP.

Working Principle

If the MAC address or OUI of an STA is in the blacklist or not in the whitelist when it goes online, the AP rejects the association request of the STA and sends an association failure response to it.

1.3.2 Configuring an SSID-based Blacklist and Whitelist

Some SSIDs may only allow specific STAs to access. In this case, you can configure an SSID-based blacklist or whitelist to prevent STAs not in the control scope to access an SSID.

To disallow or allow STAs of specific vendors to access an SSID, add the OUIs of these STAs to the OUI blacklist or whitelist of the SSID. In this case, STAs of these vendors are disallowed or allowed to access the SSID.

Working Principle

When an STA goes online through an SSID, the AP checks whether a blacklist or whitelist is configured for the SSID. If the MAC address or OUI of the STA is in the blacklist or not in the whitelist, the AP rejects the association request from the STA and sends an association failure response it.

1.3.3 Importing and Exporting Configurations

The STA access control list configuration may be large in capacity and cannot be stored together with common configuration files. You can export it to a file for backup or transfer it to another AP.

You can run an import command to import the backup configuration file to the AP to append it to the current configuration or overwrite the current configuration. Identical configurations will be merged automatically.

Working Principle

Export: Write the current configuration to the specified file in command format. The file can be exported from the AP using the **copy** command for backup or transfer.

Import: Read the specified file and import the configuration commands to the AP. In overwriting mode, configurations on the AP will be cleared in advance. In merging mode, entries in the file will be appended to the current configuration.

1.4 Configuration

Configuration	Description and Command	
Configuring an AP-based Blacklist	⚠ (Mandatory) It is used to add STAs to the AP-based blacklist.	
	blacklist mac *sta-mac*	Adds MAC addresses of STAs to the MAC address blacklist of the AP.
	blacklist vendor mac *sta-oui*	Adds OUIs of STAs to the OUI blacklist of the AP.
Configuring an AP-based Whitelist	⚠ (Mandatory) It is used to add STAs to the AP-based whitelist.	
	whitelist mac *sta-mac*	Adds MAC addresses of STAs to the MAC address whitelist of the AP.
	whitelist vendor mac *sta-oui*	Adds OUIs of STAs to the OUI whitelist of the AP.
Configuring an SSID-based Blacklist	⚠ (Mandatory) It is used to add STAs to the SSID-based blacklist.	
	blacklist mac *sta-mac* **in-ssid** *ssid-string*	Adds MAC addresses of STAs to the MAC address blacklist of an SSID.
	blacklist vendor mac *sta-oui* **in-ssid** *ssid-string*	Adds OUIs of STAs to the OUI blacklist of an SSID.
Configuring an SSID-based Whitelist	⚠ (Mandatory) It is used to add STAs to the SSID-based whitelist.	
	whitelist mac *sta-mac* **in-ssid** *ssid-string*	Adds MAC addresses of STAs to the MAC address whitelist of an SSID.
	whitelist vendor mac *sta-oui* **in-ssid** *ssid-string*	Adds OUIs of STAs to the OUI whitelist of an SSID.
Importing and Exporting Configurations	⚠ (Optional) It is used to import and export configurations.	
	export	Exports the current STA access control list configuration to a file.
	import	Imports the STA access control list configuration from a file.

1.4.1 Configuring an AP-based Blacklist

Configuration Effect

- STAs added to the MAC address blacklist cannot access all networks under the AP.
- STAs of vendors added to the OUI blacklist cannot access all networks under the AP.

Notes

- N/A

Configuration Steps

- Add MAC addresses of STAs to the MAC address blacklist of the AP.

Command	**blacklist mac** *sta-mac* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a blacklist is configured, STAs that meet the conditions are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

↘ Adding OUIs of STAs to the OUI Blacklist of the AP

Command	**blacklist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI blacklist is used to match OUIs of STAs. STAs of vendors in the OUI blacklist are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When the blacklist is enabled, an online STA that meet the conditions will be kicked offline

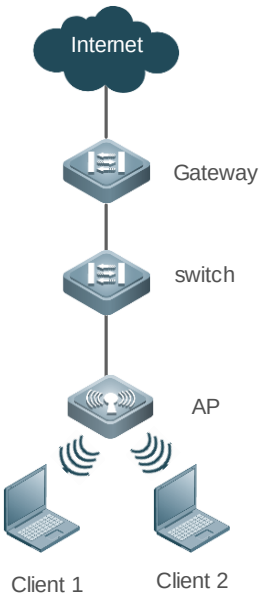
	immediately. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

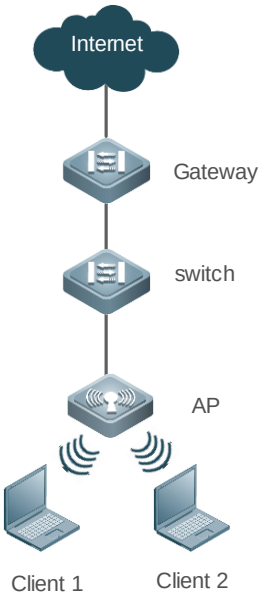
- Run the **show black-white-list blacklist** command to display the STAs in the MAC address blacklist of the AP.
- Run the **show black-white-list blacklist vendor** command to display the vendor OUIs in the OUI blacklist of the AP.

Configuration Example

↘ Configuring a MAC Address Blacklist for the AP

Scenario	
Configuration Steps	● Configure a MAC address blacklist for the AP.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist mac 0069.6c3f.2baa
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist** command. ● STAs added to the MAC address blacklist cannot associate with the AP.

Configuring an OUI Blacklist for the AP

Scenario	
Configuration Steps	● Configure an OUI blacklist for the AP.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist vendor mac 0069.6c Hostname(black-white-list)# blacklist vendor mac 0c51.01
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist vendor** command. ● STAs of vendors added to the OUI blacklist cannot associate with the AP.

Common Errors

- N/A

1.4.2 Configuring an AP-based Whitelist

Configuration Effect

- When there are entries in the MAC address whitelist, STAs not added to the whitelist cannot access any network under the AP.

- When there are entries in the OUI whitelist, STAs of vendors not added to the OUI whitelist cannot access any network under the AP.

Notes

- N/A

Configuration Steps

- Add MAC addresses of STAs to the MAC address whitelist of the AP.

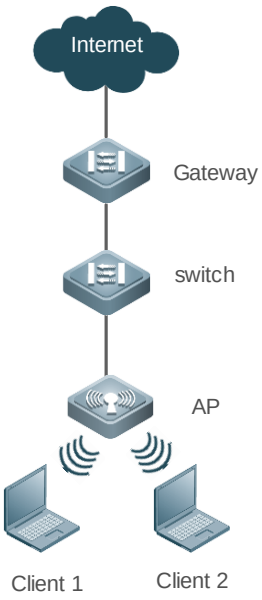
Command	**whitelist mac** *sta-mac* [**mnemonic** *string*]
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a whitelist is configured, only STAs that meet conditions are allowed to access the network. • If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When an entry is added to the whitelist, other STAs will not be kicked offline. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist** command to display the STAs in the AP-based whitelist.

Configuration Example

↘ Configuring a MAC Address Whitelist for the AP

Scenario	
Configuration Steps	● Configure a MAC address whitelist for the AP.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist mac 0069.6c3f.2baa Hostname(black-white-list)# whitelist mac 0c51.016a.5d8e
Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist** command. ● STAs not added to the whitelist cannot associate with the AP.

↘ Adding OUIs of STAs to the OUI Whitelist of the AP

Command	**whitelist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network. ● If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. ● Different types of blacklists and whitelists are complex in priority. You are advised to select a

	single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When an entry is added to the whitelist, other STAs will not be kicked offline. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Configuration Steps

↘ Adding OUIs of STAs to the OUI Whitelist of the AP

- Mandatory.

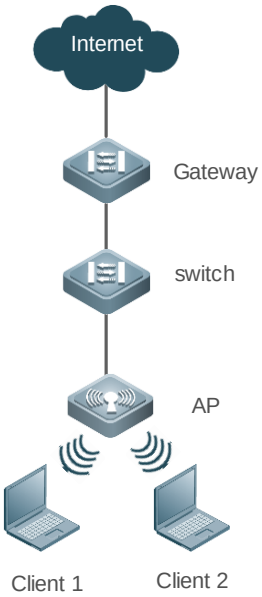
Command	**whitelist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network. ● If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. ● Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When an entry is added to the whitelist, other STAs will not be kicked offline. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist vendor** command to display the vendor OUIs in the OUI whitelist of the AP.

Configuration Example

Configuring an OUI Whitelist for the AP

Scenario	
Configuration Steps	● Configure an OUI whitelist for the AP.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist vendor mac 0069.6c Hostname(black-white-list)# whitelist vendor mac 0c51.01
Verification	● Run the **show black-white-list whitelist vendor** command to display the configuration entries. ● STAs of vendors not added to the OUI whitelist cannot associate with the AP.

Common Errors

- N/A

1.4.3 Configuring an SSID-based Blacklist

Configuration Effect

- STAs added to the MAC address blacklist of an SSID cannot access the SSID.

- When there are entries in the OUI blacklist of the specified SSID, STAs of vendors added to the OUI blacklist cannot access the SSID.

Notes

N/A

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Blacklist of the Specified SSID

Command	**blacklist mac** *sta-mac* **in-ssid** *ssid* [**mnemonic** *string*]
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a blacklist is configured, STAs that meet the conditions are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list blacklist in-ssid** *ssid* command to display the STAs in the blacklist of the SSID.

↘ Adding OUIs of STAs to the OUI Blacklist of the Specified SSID

-

Command	**blacklist vendor mac** *sta-oui* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI blacklist is used to match OUIs of STAs. STAs of vendors in the OUI blacklist are not allowed to access the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a

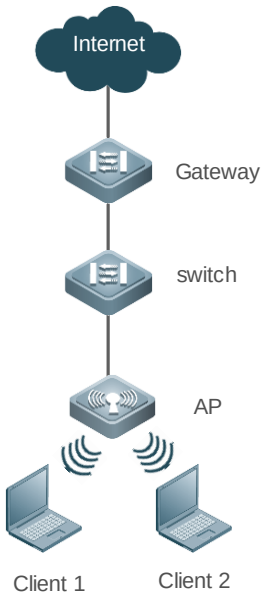
	single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list blacklist vendor in-ssid** *ssid* command to display the OUIs of vendors in the OUI blacklist of the SSID.

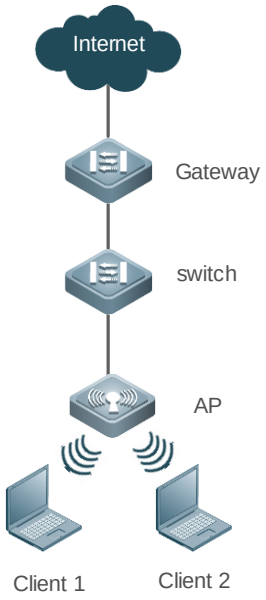
Configuration Example

↘ Configuring a MAC Address Blacklist for an SSID

Scenario	
Configuration Steps	● Configure a MAC address blacklist for SSID Hostname-web.
	HOSTNAME# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist mac 0069.6c3f.2baa in-ssid Hostname-web
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist in-ssid** *ssid-string* command.

	● STAs added to the blacklist cannot associate with the SSID.

Configuring an OUI Blacklist for an SSID

Scenario	
Configuration Steps	● Configure an OUI blacklist for SSID Hostname-web.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# blacklist vendor mac 0069.6c in-ssid Hostname-web Hostname(black-white-list)# blacklist vendor mac 0c51.01 in-ssid Hostname-web
Verification	● Configuration entries are displayed in the output of the **show black-white-list blacklist vendor in-ssid** *ssid-string* command. ● STAs of vendors added to the blacklist cannot associate with the SSID.

Common Errors

- N/A

1.4.4 Configuring an SSID-based Whitelist

Configuration Effect

- When there are entries in the MAC address whitelist of the specified SSID, STAs not added to the MAC address whitelist cannot access the SSID.

- When there are entries in the OUI whitelist of the specified SSID, STAs of vendors not added to the OUI whitelist cannot access the SSID.

Notes

- N/A

Configuration Steps

↘ Adding MAC Addresses of STAs to the MAC Address Whitelist of the Specified SSID

Command	**whitelist mac** *sta-mac* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• After a whitelist is configured, only STAs that meet conditions are allowed to access the network. • If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. • Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. • The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. • Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. • When an entry is added to the whitelist, other STAs will not be kicked offline. • In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist in-ssid** *ssid* command to display the STAs in the whitelist of the SSID.

↘ Adding OUIs of STAs to the OUI Whitelist of the Specified SSID

Command	**whitelist vendor mac** *sta-oui* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	*N/A*
Defaults	No entry is configured by default.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network. • If the whitelist is empty, all STAs are allowed to access the network. If there is data in the

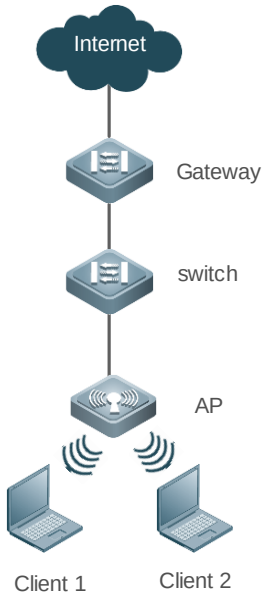
	whitelist, STAs not listed in the whitelist are immediately banned from accessing the network. ● Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device. ● Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types. ● When an entry is added to the whitelist, other STAs will not be kicked offline. ● In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

Verification

- Run the **show black-white-list whitelist vendor in-ssid** *ssid* command to display the OUIs of vendors in the OUI whitelist of the SSID.

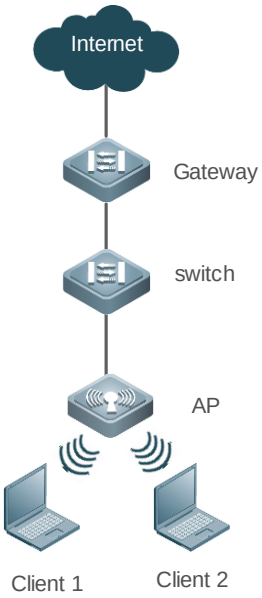
Configuration Example

↘ Configuring a MAC Address Whitelist for an SSID

Scenario	
Configuration Steps	● Configure a MAC address whitelist for SSID Hostname-web.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist mac 0069.6c3f.2baa in-ssid Hostname-web Hostname(black-white-list)# whitelist mac 0c51.016a.5d8e in-ssid Hostname-web

Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist in-ssid** *ssid-string* command. ● STAs not added to the MAC address whitelist cannot associate with the SSID.

↘ Configuring an OUI Whitelist for an SSID

Scenario	
Configuration Steps	● Configure an OUI whitelist for SSID Hostname-web.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# whitelist vendor mac 0069.6c in-ssid Hostname-web Hostname(black-white-list)# whitelist vendor mac 0c51.01 in-ssid Hostname-web
Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist vendor in-ssid** *ssid-string* command. ● STAs of vendors not added to the OUI whitelist cannot associate with the SSID.

Common Errors

- N/A

1.4.5 Importing and Exporting Configurations

Configuration Effect

- Export the current STA access control list configuration to a file.
- Import the STA access control list configuration from a file. You can select whether the imported configuration is appended to or overwrites the current configuration. If you select overwriting, clear the current configuration before importing the configuration. If you select merging, the configuration in the file will be appended to the current configuration.

Notes

- If the flash memory is insufficient during configuration export, a failure prompt is displayed.

Configuration Steps

↘ Exporting the Current Configuration to a File

- This command takes effect only once and is not saved.

Command	**export**
Parameter Description	*N/A*
Defaults	N/A
Command Mode	STA access control list configuration mode
Usage Guide	The configuration will be exported to the **black-white-list.csv** file. You can run the **copy** command to upload the file to a PC and use Excel to edit it.

↘ Importing the Configuration from a File

- This command takes effect only once and is not saved.

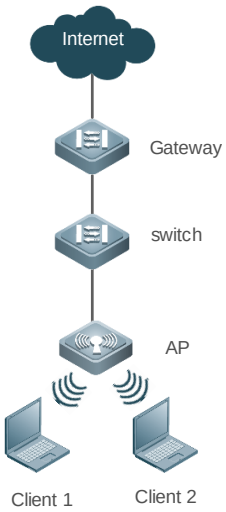
Command	**import** *filename* **{replace | append}**
Parameter Description	*N/A*
Defaults	N/A
Command Mode	STA access control list configuration mode
Usage Guide	N/A

Verification

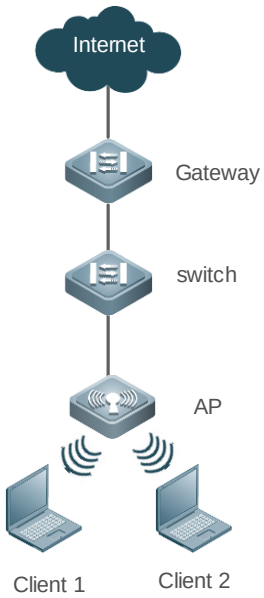
- Run the **show black-white-list config** command to display the configurations.
- Run the **dir** command to display files in the flash memory.

Configuration Example

↘ Exporting the Current Configuration to a File

Scenario	
Configuration Steps	● Export the current configuration to the **black-white-list.csv** file.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# export 10 entrys successfully exported.
Verification	● Run the **dir** command. The **black-white-list.csv** file is displayed in the output of the **dir** command. ● Run the **more black-white-list.csv** command. The file content is the STA access control list configuration.

Importing the Configuration from a File

Scenario	

Configuration Steps	● Import the configuration from the **black-white-list.csv** file and append it to the current configuration.
	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# black-white-list Hostname(black-white-list)# import black-white-list.csv append
Verification	● Run the **show black-white-list config** command to display the configurations.

Common Errors

- N/A

1.5 Monitoring

Clearing

Description	Command
Clears entries in the MAC address blacklist of an AP or SSID.	**reset blacklist** [**in-ssid** *ssid-string*]
Clears entries in the MAC address whitelist of an AP or SSID.	**reset whitelist** [**in-ssid** *ssid-string*]
Clears entries in the OUI whitelist of an AP or SSID.	**reset whitelist vendor** [**in-ssid** *ssid-string*]
Clears entries in the OUI blacklist of an AP or SSID.	**reset blacklist vendor** [**in-ssid** *ssid-string*]

Displaying

Description	Command
Displays basic information of an STA access control list.	**show black-white-list summary**
Displays the STA access control list configuration.	**show black-white-list config**
Displays STAs in both the blacklist and whitelist.	**show black-white-list conflict**
Displays the blacklist/whitelist configuration type of a specific STA.	**show black-white-list sta-mac** *sta-mac*
Displays entries in the MAC address blacklist of an AP or SSID.	**show black-white-list blacklist** [**in-ssid** *ssid-string*]
Displays entries in the OUI blacklist of an AP or SSID.	**show black-white-list blacklist vendor** [**in-ssid** *ssid-string*]
Displays entries in the MAC address whitelist of an AP or SSID.	**show black-white-list whitelist** [**in-ssid** *ssid-string*]

Displays entries in the OUI whitelist of an AP or SSID.	**show black-white-list whitelist vendor** [**in-ssid** *ssid-string*]

Debugging

N/A

1 Configuring WIDS

1.1 Overview

Compared with wired networks, Wireless LAN (WLAN) has unparalleled advantages, such as convenient deployment, flexible use, efficient cost, and easy extension, making it more and more prevalent. However, for the openness of its channels, WLAN is much vulnerable to various network threats, such as rogue access points (APs), Ad-hoc networks, and all types of protocol attacks. Therefore, security becomes a major factor that hinders WLAN development.

Wireless Intrusion Detection System (WIDS) detects vicious STA attacks and invasions in the early stage, which helps network administrators actively observe and defend against the hidden dangers in networks in the first time.

1.2 Applications

Application	Description
Frame Filtering	Facing illegal STAs attempting to access WLAN, WIDS frame filtering helps control STA access.
User Isolation	Facing a STA intending to visit other STAs in WLAN, WIDS user isolation helps isolate their direct communication.
IDS	Facing all kinds of invasion attacks in WLAN, Intrusion Detection System (IDS) helps detect those attacks.
Rogue Detection and Containment	Illegal or rogue devices in WLAN jeopardize STAs and normal services by faking services. Facing it, Rogue detection and containment help monitor and contain them.

1.2.1 Frame Filtering

Scenario

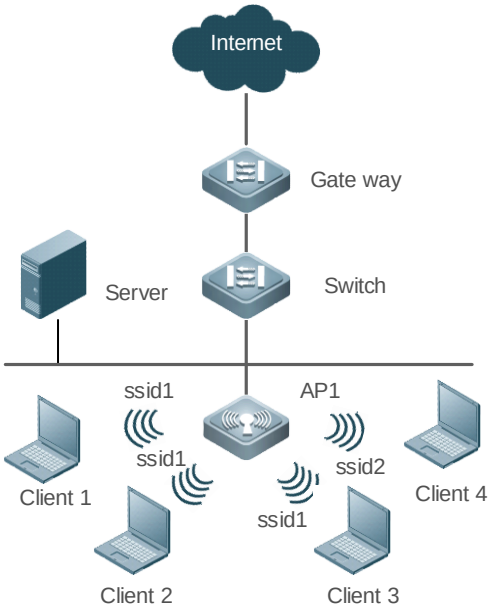
The wireless access control service is provided in WLAN, including allowing specified STAs to access WLAN or specified networks, forbidding STAs from accessing WLAN or specified networks, forbidding low-rate stations (STAs) from accessing WLAN, as well as dynamically controlling network access.

The figure below is an example, assuming that there are the following deployment requirements in the network:

- Allow Client 1 to access WLAN and Client 2 to access SSID 1.
- Prohibit Client 3 from accessing WLAN and Client 4 from accessing SSID 2.
- Filter and kick out low-rate STAs.
- Dynamically control STA access.

The networking topology is shown as follows:

Figure 1-1 Networking Topology of Wireless Access Control



Deployment

The key configuration points for the devices are:

- Add Client 1 to a WIDS whitelist. As a result, Client 1 can access the WLAN service provided by AP. Other STAs not in the list cannot.
- Add Client 2 to the SSID 1-based whitelist. As a result, Client 2 can access SSID 1 provided by AP. Other STAs not in the list cannot.
- Add Client 3 to a static blacklist. As a result, Client 3 cannot access the WLAN service provided by AP.
- Add Client 4 to the SSID 1-based blacklist. As a result, Client 4 cannot access SSID 1 provided by AP.
- Configure the low-rate threshold. STAs with rates less than the threshold will be kicked out.
- Enable the dynamic blacklist function, supporting the IDS function. After the dynamic blacklist function is enabled, any detected attack will be added into the dynamic blacklist. When the blacklist is within aging duration, the listed STAs will continue to be forbidden from communication accessed by the current AP.

1.2.2 User Isolation

Scenario

Layer 2 user isolation is provided on a WLAN, including AP-based, AP-SSID-based, AC-based, AC-SSID-based, and SSID-based user isolation.

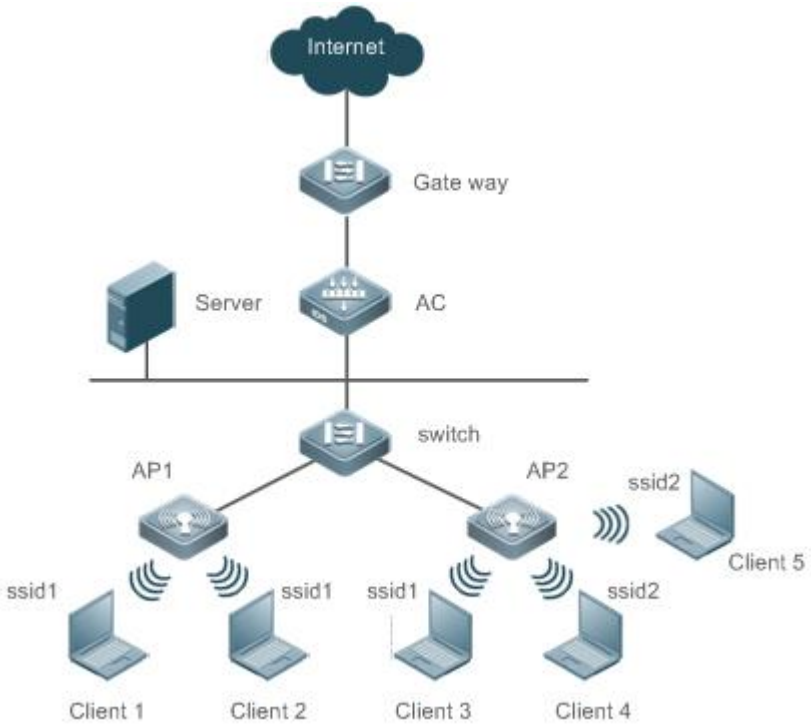
Provided that the following deployment requirements should be met on a WLAN:

1. Client 1 to Client 3 are associated with SSID 1, and Client 4 and Client 5 are associated with SSID 2. SSID 1 and SSID 2 are mapped to the same VLAN. Client 1 to Client 5 are Layer 2 users.

1. Direct communication cannot be conducted between Client 1 and Client 2, and among Client 3, Client 4 and Client 5, but can be done among other users.
2. Direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5, but can be done among other users.
3. Direct communication cannot be conducted between Client 1 and Client 3, Client 4, or Client 5, and between Client 2 and Client 3, Client 4, or Client 5, but can be done among other users.
4. Direct communication cannot be conducted between Client 3 and Client 1 or Client 2, but can be done among other users.
5. Direct communication cannot be conducted among Client 1, Client 2, and Client 3, but can be done among other users.

The networking topology is shown as follows:

Figure 1-2 Networking Topology of Wireless User Isolation



Deployment

The key configuration points for the devices are:

- Configure AP-based user isolation. As a result, direct communication can be conducted between Client 1 and Client 2, and among Client 3, Client 4, and Client 5.
- Configure AP-SSID-based user isolation. As a result, direct communication can be conducted between Client 1 and Client 2, and between Client 4 and Client 5.
- Configure AC-based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 3, Client 4, or Client 5, and between Client 2 and Client 3, Client 4, or Client 5.
- Configure AC-SSID-based user isolation. As a result, direct communication can be conducted between Client 3 and Client 1 or Client 2.

- Configure SSID1-based user isolation. As a result, direct communication cannot be conducted among Client 1, Client 2, and Client 3.

1.2.3 IDS

Scenario

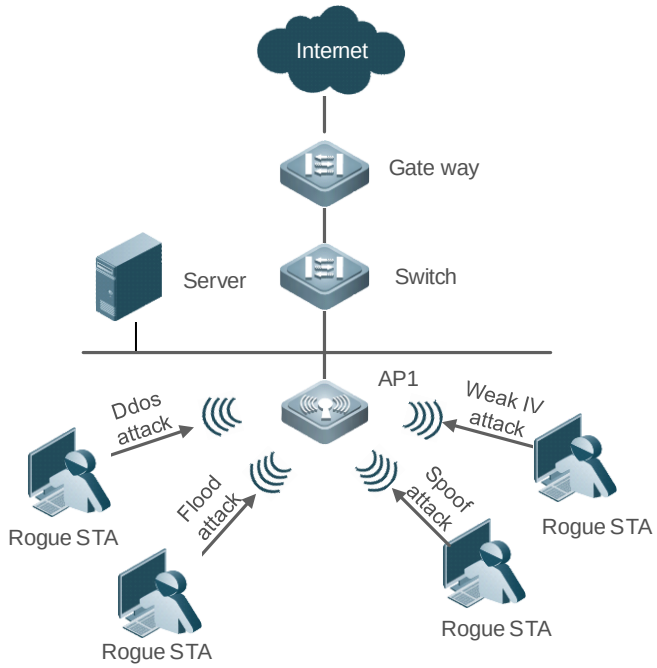
Wireless invasion attacks exist in networks, including Distributed Denial of Service (DDoS), spoofing, flooding, and Weak IV attacks. It requires APs to detect these attacks and carry out countermeasures.

Assuming there are the following deployment requirements in the network:

- DDoS attacks
- Spoofing attacks
- Flooding attacks
- Weak IV attacks

The networking topology is shown as follows:

Figure 1-3 Networking Topology of IDS



Deployment

The key configuration points for the devices are:

- Enable DDoS detection with thresholds specified which perform statistics of ARP, SYN and ICMP attack packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.

- Enable the spoofing detection with related thresholds specified to detect the deauthentication and disassociation packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable flooding detection with related thresholds specified to detect the Authentication, Association, Reassociation, Deauthentication, Disassociation, Probe, Null data and Action packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable the Weak IV detection with related thresholds specified to detect the IV value of the Web packets. If the number of continuous attacks exceeds the threshold, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.

1.2.4 Rogue Detection and Containment

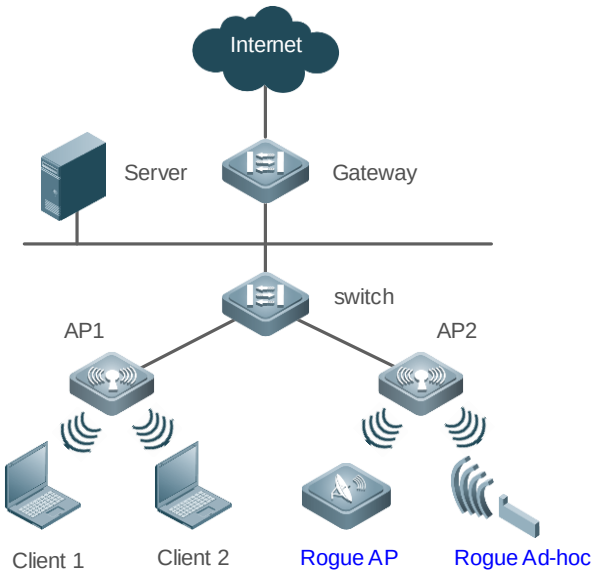
Scenario

Assuming there is the following deployment requirement in the network:

- Rogue AP and Ad-hoc devices exist in network, and detection and containment are required.

The networking topology is shown as follows:

Figure 1-4 Networking Topology of Rogue Detection and Containment



Deployment

The key configuration points for devices are:

- Enable the Monitor or Hybrid mode for a specified AP, and start the detection timer of the AP and obtain detected data at the end of each period.
- Enable the device containment and configure the mode.
- Counter the Rogue APs and Ad-hoc devices regularly based on the containment mode and detected data, preventing users from associating with fake services.

- Before the configured AP containment takes effect, confirm that WLAN is available for the AP; otherwise, the containment function will lose effect.

1.3 Features

Basic Concepts

Working Modes

The WIDS has the following working modes:

- Normal mode, providing only the access service
- Monitor mode, providing only the monitoring service
- Hybrid mode, providing both monitoring and access services

IDS Detection Types

The IDS attack detection has the following types:

- DDoS attack detection, detecting DDoS attacks involving ARP, ICMP and SYN packets
- Flooding attack detection, detecting the flooding attacks involving single-user or multi-user management packets
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication attacks
- Weak IV attack detection, detecting weak vector attacks

User Isolation Modes

The user isolation has the following modes:

- AP-based: Communication cannot proceed between layer-2 users under the same AP.
- AP-SSID based: Communication cannot proceed between layer-2 users under the same AP and in the same WLAN.
- SSID-based: Communication cannot proceed between layer-2 users in specified WLAN.

Rogue Containment Modes

The Rogue containment has the following modes:

- Ad-hoc containment mode, containing the Rogue Ad-hoc devices
- Rogue containment mode, containing the Rogue devices with over-limit RSSI
- SSID containment mode, containing illegal devices with the same SSID
- Config containment mode, containing the illegal devices in the static attack list or the SSID blacklist

Fuzzy Containment on Rogue APs

- Fuzzy match is performed based on the SSID of the rogue AP. For example, if the SSID of the local host is RUIJIE-WEB, the rogue AP whose SSID is RU1JIE-WEB can be contained after the fuzzy containment function is enabled.

- Fuzzy containment can be performed by keyword. For example, if the configured fuzzy containment keyword is ruijie, rogue APs whose SSIDs contain ruijie such as ruijie-free can be contained after the fuzzy containment function is enabled. The keyword is case-insensitive. For example, assume that the keyword is ruijie. There are 2^6 uppercase and lowercase combinations of ruijie. Once the fuzzy containment keyword is set to any of the combinations, APs whose SSIDs contain any combination of ruijie can be identified, such as RUIjie and RuiJie.

↘ Detected Devices

The types of detected rogue devices are as follows:

- APs
- Ad-hoc devices
- Unknown STAs

Overview

Feature	Description
Frame Filtering	Certain filtering rules are used to filter the packets from STAs for access control.
IDS	Timely discovers and defends against malicious or unintentional attacks in WLAN.
User Isolation	Interdicts the insecure access between STAs in WLAN to prevent disclosure of private information.
Rogue Detection and Containment	Monitors abnormal devices in the whole WLAN, helping the network administrators find hidden dangers in networks. Rogue containment refers to containing Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices in a blacklist.

1.3.1 Frame Filtering

The access control over STAs includes: low-rate filter, whitelist, static blacklist, dynamic blacklist, SSID-based whitelist and SSID-based blacklist.

Working Principle

↘ Low-Rate Filter

The low-rate filter sets a kickout threshold. When the threshold is larger than 0, the filter is enabled. If the STA rate is lower than this threshold, the STA's packets will be discarded and this STA will be disconnected.

↘ Allowlist

The whitelist includes MAC addresses of admitted STAs. If the whitelist function is enabled, only the whistlisted can access the WLAN. Other STAs will be forced to go offline and cannot access the WLAN, so as to reduce the impact of illegal packets in the WLAN.

↘ Static Blocklist

The static blacklist includes MAC address of the denied STAs. If the static blacklist function is enabled, STAs in the blacklist will be forced to go offline and cannot access the network.

Dynamic Blocklist

The dynamic blacklist includes MAC addresses of the denied STAs. You can configure the dynamic blacklist if DDoS attacks are detected. For example, add the MAC address of a detected attacker into the blacklist dynamically to forbid receiving any packet from it, thereby ensuring WLAN security.

SSID-based Allowlist

The SSID-based whitelist includes MAC addresses of the STAs admitted into a WLAN with a specified SSID. You can configure the SSID-based whitelist. If the SSID-based whitelist function is enabled, only the STAs in the whitelist of the specified WLAN are allowed to access. Other STAs cannot access the specified WLAN and online STAs that are not in the whitelist will be forced to go offline, so as to reduce the impact of illegal packets in WLAN.

SSID-based Blocklist

The SSID-based blacklist includes MAC addresses of the STAs denied by a WLAN with a specified SSID. You can configure the SSID-based blacklist. If the SSID-based blacklist function is enabled, STAs in the blacklist will be forced to go offline and cannot access this WLAN.

1.3.2 IDS

In order to timely find and defend against malicious or unintentional attacks in WLAN, IDS supports the detection on multiple attacks. When an attack is detected, an alert or a log will be generated to remind the network administrator of treatment. Based on detected results, the network administrator can timely adjust network configuration to clear the insecure factors in WLAN.

Currently, devices support the following types of IDS attack detection:

- DDoS attack detection
- Flooding attack detection
- Spoofing attack detection
- Weak IV detection

Working Principle

DDoS Attack Detection

DDoS attack means that the attackers send a large number of attack packets toward targeted devices in a short period of time (ARP packets, ICMP packets and SYN packets identified currently) so as to affect legal STAs being associated with the attacked device.

DDoS detection function performs statistics for the attacker's packets and determines whether the number of packets per second exceeds the configured threshold. If yes, this result will be logged. If the dynamic blacklist function is enabled, the attacker will be added into the dynamic blacklist.

Flooding Attack Detection

Flooding attack refers to that an attacker sends a large number of packets of the same type in a short period of time, causing the WLAN devices fail to process legal STA requests due to the Rogue flooding.

Flooding attack detection prevents this flooding attack by continuously monitoring the traffic of each device. Within specified time, when the traffic exceeds the upper limit set by the network administrator, this device is deemed to be a flooding attacker and is therefore blocked. Flooding attack detection can be used with the dynamic blacklist function. When attacks are detected, if the dynamic blacklist function is enabled, the STA initiating the attacks will be added into the dynamic blacklist, ensuring no more intrusion by this STA and thus guaranteeing network security.

↘ Spoofing Attack Detection

Spoofing attack refers to that an attacker sends fake packets in the name of another STA. For example, a fake deauthentication packet causes a STA offline.

WIDS performs detection on the broadcast deauthentication and broadcast disassociation packets. When such packet is received, it is immediately defined as a spoofing attack and logged.

↘ Weak IV Attack Detection

Weak IV (Weak Initialization Vector) attack refers to the following attack behavior: when the WLAN uses WEP encryption, an attacker intercepts packets with weak initialization vectors, cracks the shared key and finally steals the encrypted information.

When WLAN uses WEP for encryption, an initialization vector (IV) is generated for each packet and, together with the shared key, taken as input to generate a key string. With the key string and plain-text encryption, the cipher text is generated finally. When a WEP packet is sent, the IV used for packet encryption is also taken as a part of the packet header to be sent. If the IV is generated with an insecure method, for example, repetitive IVs are frequently generated or even the same IV is always generated, the shared key will be exposed easily. If a potential attacker obtains the shared key, it can control network resources and pose a threat to network security.

The IDS prevents this attack by identifying the IV of each WEP packet. When a packet with a weak IV is detected, the IDS immediately determines that this is vulnerability and logs this detected result.

1.3.3 User Isolation

Because of the mobility and uncertainty of STAs, STA information privacy appears to be particularly important in some occasions (especially public areas). Therefore, direct STA communication should be restricted. The user isolation technology can avoid insecure access between STAs in WLAN coverage (e.g., via online neighborhood), so as to prevent private information from being stolen by others.

User isolation isolates STAs, and prevents them from accessing each other without affecting their normal network access, guaranteeing service security. The layer-2 user isolation has the following types:

- AP-based user isolation
- AP-SSID based user isolation

Working Principle

↘ AP-Based User Isolation

Direct communication cannot be conducted between layer-2 STAs associated with the same AP.

AP-SSID based User Isolation

Direct communication cannot be conducted between STAs in the same WLAN who are associated with the same AP.

1.3.4 Rogue Detection and Containment

Network devices are usually divided into two types: illegal (Rogue) and legal. Rogue devices have potential vulnerabilities to be attacked or manipulated, which therefore poses a serious threat or hazard to network security. Rogue detection function can monitor abnormal devices in the whole WLAN, helping the network administrator find hidden dangers in networks.

Rogue detection is applicable to multiple Rogue devices in WLAN: APs, clients, wireless bridges, and Ad-hoc devices. Currently, only the detection on Rogue APs and Ad-hoc devices and unknown STAs is supported.

Rogue device containment counters Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices, as so to prevent STAs from accessing illegal service or illegal STAs from accessing the devices.

Working Principle

Rogue Detection

The Rogue detection function is conducted by an AP in Monitor mode or Hybrid mode. WIDS captures wireless packets in the air by deploying some APs in WLAN and setting them to operate in Monitor or Hybrid mode. By conducting analysis and statistics of monitored wireless packets, the AP can obtain information on the Rogue device. Meanwhile, the network administrator can also prepare illegal device detection rules to monitor abnormal devices in the whole WLAN.

Unknown STA Detection

The unknown STA detection function monitors the probe request packets from non-accessed STAs in the network, and the network administrator can also use configuration to specify information on the unknown STA.

Rogue Containment

The Rogue containment refers to a service which uses the means of simulating fake broadcast deauthentication packets to contain Rogue devices that meet the containment mode rules, and to prevent normal STAs from accessing Rogue devices.

Unknown STA Containment

The unknown STA containment refers to denying unknown STA access by directly constructing deauthentication packets.

1.4 Configuration

Configuration	Description and Command	
Configuring Frame Filtering	⚠ (Optional) It is used to configure frame filtering.	
	kickout threshold	Configures the low-rate kickout threshold.

Configuration	Description and Command	
	whitelist mac-address [**name** *another-name*]	Adds an entry to the whitelist.
	whitelist max	Configures the length of the whitelist.
	static-blacklist mac-address [**name** *another-name*]	Adds an entry to the static blacklist.
	static-blacklist max	Configures the length of the static blacklist.
	dynamic-blacklist enable	Enables the dynamic blacklist function.
	dynamic-blacklist lifetime	Configures the lifetime of the dynamic blacklist.
	dynamic-blacklist ap-max	Configures the length of the dynamic blacklist on APs.
	ssid-filter max	Configures the SSID-based blacklist and whitelist and their length.
	ssid-filter blacklist mac-address [**name** *another-name*]	Adds an entry to the SSID-based blacklist.
	ssid-filter blacklist max	Configures the length of the SSID-based blacklist, 256 by default.
	ssid-filter whitelist mac-address [**name** *another-name*]	Adds an entry to the SSID-based whitelist.
	ssid-filter whitelist max	Configures the length of the SSID-based whitelist, 256 by default.
Configuring IDS	⚠ (Mandatory) It is used to configure IDS.	
	attack-detection enable	Specifies the IDS type.
	attack-detection ddos	Configures the interval and packet threshold of DDoS attack detection.
	attack-detection flood multi-mac	Configures the interval and packet threshold of multi-STA flooding attack detection.
	attack-detection flood single-mac	Configures the interval and packet threshold of single-user flood attack detection.
	attack-detection spoof	Configures the interval and packet threshold of the spoofing attack detection.
	attack-detection weak-iv	Configures the interval and packet threshold of the weak IV attack detection.
	attack-detection statistics ap-max	Configures the length of IDS statistics on APs.
Configuring User Isolation	⚠ (Optional) It is used to configure user isolation.	
	user-isolation enable	Enables the AC-based, AP-based, AC-SSID-based, AP-SSID-based and CMCC layer-2 user isolation.
	user-isolation permit-mac	Adds an entry to the permissible MAC list for user isolation.

Configuration	Description and Command	
	user-isolation permit-mac max	Configures the length of the permissible MAC list for user isolation.
Configuring Rogue Detection and Containment	⚠ (Optional) It is used to set the device detection and containment function.	
	countermeasures enable	Enables the Rogue containment function.
	countermeasures ap-max	Configures the maximum number of contained devices once.
	countermeasures channel-match	Enables channel-based containment.
	countermeasures interval	Configures the containment interval.
	countermeasures mode	Configures the containment mode.
	countermeasures rssi-min	Configures the minimum containment RSSI.
	countermeasures fuzzy-enable	Enables fuzzy containment.
	countermeasures fuzzy-keyword	Configures a fuzzy containment keyword.
	device aging duration	Configures the aging duration of the detected devices.
	device attack mac-address	Adds an entry to the static attack list.
	device attack max	Configures the length of the static attack list.
	device black-ssid	Adds an entry to the SSID-based blacklist.
	device max-black-ssid	Configures the length of the SSID-based blacklist.
	device friendly-flags	Configures the device friendly flag.
	device permit mac-address	Adds an entry to the permissible MAC list.
	device permit mac-address max	Configures the length of the permissible MAC list.
	device permit ssid	Adds an entry to the permissible SSID list.
	device permit max-ssid	Configures the length of the permissible SSID list.
	device permit vendor bssid	Adds an entry to the permissible vendor list.
	device permit vendor bssid max	Configures the length of the permissible vendor list.
	device unknown-sta dynamic-enable	Enables unknown STA detection and containment.
	device unknown-sta mac-address	Adds an entry to the unknown STA list
	device unknown-sta mac-address max	Configures the length of the unknown STA list.
	device unknown-sta report enable	Enables unknown STA detection information reporting.
	device channel-bind radio	Configures the scanning channel of a specified radio.
	device detected-ap-max	Configures the maximum number of detected APs.

Configuration	Description and Command	
	hybrid-scan radio	Configures the scanning status of a specified radio.
	scan-channels { 802.11a | 802.11b | 6GHz} channels	Configures the scanning channel of a specified AP.
	scan-channels { dual-band | all-band }	Configures automatic dual-radio switchover and scanning.
Configuring AP Working Mode	⚠ (Optional) It is used to set the AP working mode.	
	device mode	Configures the AP working mode.

1.4.1 Configuring Frame Filtering

Configuration Effect

- Configure the frame filtering rules to provide packet filtering services.

Notes

- A STA cannot be configured in both the static blacklist and the whitelist.
- A STA cannot exist in both the blacklist and whitelist of the same SSID.

Configuration Steps

↘ Configuring the Low-Rate Filter

- (Optional) The **kickout threshold** command is used in WIDS configuration mode to configure the low-rate kickout threshold. The low-rate filtering function effectively works only after the low-rate kickout threshold is configured (larger than 0).
- Unless otherwise noted, enable this function only on devices which needs to support the low-rate STA filtering function.

Command	**kickout threshold** *rate*
Parameter Description	*rate*: Indicates the low-rate kickout threshold ranging from 0 to 130 Mbps.
Defaults	By default, low-rate STAs are not filtered out, and the kickout threshold is 0.
Command Mode	WIDS configuration mode
Usage Guide	The STAs can select different low-rate STA filtering thresholds based on requirements.

↘ Configuring the STA Disconnection Function

- (Optional) The **kickout client** command is used in WIDS configuration mode to disconnect online STAs.

Command	**kickout client** *H.H.H*
Parameter Description	*H.H.H*: Indicates the MAC address of a STA that is disconnected.

Defaults	N/A
Command Mode	WIDS configuration mode
Usage Guide	This command can be used to disconnect a specified online STA.

Configuring the Allowlist

- Optional.
- Run the **whitelist mac-address** command to add an entry to the whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **whitelist max** command to configure the maximum number of entries in the whitelist in WIDS configuration mode.
- If the address whitelist is configured, all online STAs whose addresses are not in the whitelist will be forced to go offline 1 minute after the last configuration command is executed.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**whitelist** { **mac-address** *H.H.H* [**name** *another-name*] | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a whitelist entry. **name** *another-name*: Indicates the another-name of the MAC address in the whitelist. **max** *num*: Indicates the length of the whitelist ranging from 1 to 2,048.
Defaults	By default, the whitelist is empty and the whitelist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The whitelist function takes effect only when the whitelist has entries.

Configuring the Static Blocklist

- Optional.
- Run the **static-blacklist mac-address** command to add an entry to the static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **static-blacklist max** command to configure the maximum number of entries in the static list in WIDS configuration mode, indicating the maximum number of permissible static blacklist entries on the device.
- After the MAC address of a STA is added to the static blacklist, the STA will be forced to go offline immediately if the STA is online.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**static-blacklist** { **mac-address** *H.H.H* [**name** *another-name*] | **max** *num* }

Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static blacklist entry. **name** *another-name*: Indicates the another-name of the MAC address in the static blacklist. **max** *num*: Indicates the length of the static blacklist ranging from 1 to 2,048.
Defaults	By default, the static blacklist is empty and the static blacklist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The static blacklist function takes effect only when the static blacklist has entries.

Configuring the Dynamic Blocklist

- Optional.
- Run the **dynamic-blacklist enable** command to enable the dynamic blacklist function in WIDS configuration mode. A dynamic blacklist entry is generated dynamically along with the IDS attack detection and works only after the dynamic blacklist function is enabled.
- Run the **dynamic-blacklist lifetime** command to configure the service life of the dynamic blacklist in WIDS configuration mode, indicating how long the dynamic blacklist exists in the device.
- Run the **dynamic-blacklist ap-max** command to configure the maximum number of dynamic blacklist entries on APs in WIDS configuration mode.
- Run the **dynamic-blacklist mac-adress** command to configure the dynamic blocklist in WIDS configuration mode.

Command	**dynamic-blacklist** { **enable** | **lifetime** *time* | **ap-max** *num* }
Parameter Description	**enable**: Enables the dynamic blacklist function **lifetime** *time*: Indicates the service life of the dynamic blacklist ranging from 60 to 86,400 seconds. **ap-max** *num*: Indicates the length of the dynamic blacklist on APs.
Defaults	By default, the dynamic blacklist function is disabled. The default length of the dynamic blacklist is 4,096 with 300-second lifetime.
Command Mode	WIDS configuration mode
Usage Guide	A dynamic blacklist entry is generated in the IDS attack detection function.

Configuring the SSID-Based Blocklist

- Optional.
- Run the **ssid-filter blacklist mac-address** command to add an entry to the SSID-based static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **ssid-filter blacklist max** command to configure the maximum number of entries in the SSID-based static blacklist in WIDS configuration mode.
- After the MAC address of a STA is added to the blacklist, the STA will be forced to go offline immediately if the STA is online and associated with the SSID.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.

- The another-name is null if it is not configured.

Command	**ssid-filter** { **max** *num* | **blacklist mac-address** *H.H.H* [**name** *another-name*] **in-ssid** *string* | **blacklist max** *num* }
Parameter Description	**max** *num*: Indicates the maximum length of the SSID-based blacklist, ranging from 1 to 128. The default is 64. **blacklist mac-address** *H.H.H* **in-ssid** *string*: Adds an entry to the specified SSID-based blacklist. **name** *another-name*: Indicates the another-name of the MAC address in the specified SSID blacklist. **blacklist max** *num*: Configures the length of the SSID-based blacklist, ranging from 1 to 2048.
Defaults	The SSID-based blacklist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based blacklist has entries. The maximum number of the SSID blacklist is 32768. To change the value of **ssid-filter blacklist max**, please ensure the product of **ssid-filter max** and **ssid-filter blacklist max** is smaller than 32768. For example, if the value of **ssid-filter blacklist max** is 2048, then the value of **ssid-filter max** can not exceed 16.

Configuring the SSID-Based Allowlist

- Optional.
- To configure the SSID-based whitelist entry, the same as above.
- To configure the SSID-based whitelist length, the same as above.
- Run the **ssid-filter whitelist mac-address** command to add an entry to the SSID-based whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **ssid-filter whitelist max** command to configure the maximum number of entries in the SSID-based whitelist in WIDS configuration mode.
- After the SSID-based whitelist is configured, STAs that are not in the whitelist of this SSID will be forced to go offline.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**ssid-filter** { **whitelist mac-address** *H.H.H* [**name** *another-name*] **in-ssid** *string* | **whitelist max** *num* }
Parameter Description	**whitelist mac-address** *H.H.H* **in-ssid** *string*: Configures the whitelist entry for a specified SSID. **name** *another-name*: Indicates the another-name of the MAC address in the specified SSID whitelist. **whitelist max** *num*: Configures the length of the SSID-based whitelist, ranging from 1 to 2048.
Defaults	The SSID-based whitelist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based whitelist has entries.

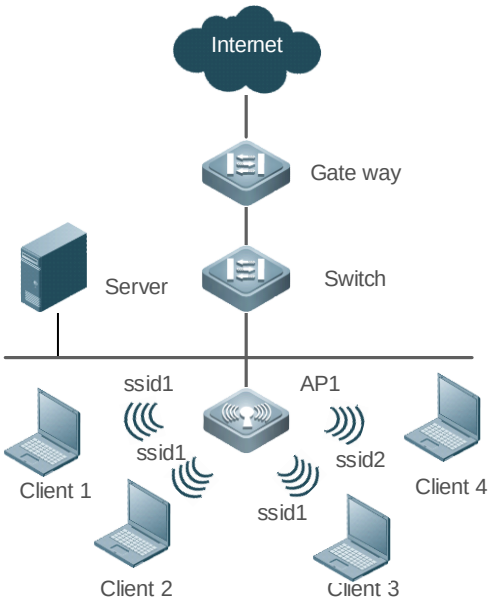
Verification

Conduct related function verifications based on corresponding frame filtering rules.

- Check the low-rate STA filtering function. The packets are discarded and the low-rate STAs are successfully removed.
- Check the whitelist function. When the whitelist is configured, the STAs not included in the whitelist cannot join the AP.
- Check the static blacklist function. When the static blacklist is configured, the STAs included in the static blacklist cannot join the AP.
- Check the dynamic blacklist function. When the dynamic blacklist function is enabled, entries in the dynamic blacklist can be generated along with the IDS attack detection, and STAs in the dynamic blacklist cannot join the AP again.
- Check the SSID-based blacklist function. When the SSID-based blacklist is configured, STAs in the SSID-based blacklist cannot join this SSID service.
- Check the SSID-based whitelist function. When the SSID-based whitelist is configured, STAs not included in the SSID-based whitelist cannot join this SSID service.

Configuration Example

↘ Configuring the Allowlist Entry

Scenario **Figure 1-5**	
Configuration Steps	● Add an entry to the whitelist on AP.
	Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# whitelist mac-address 0000.0000.0001
Verification	After the STA configures the whitelist entry, the following methods can be used to check the

	configuration. ● Run the **show wids whitelist** command to display the information on related parameters configured on the STA. ● Use the device to verify whether the function has taken effect.
	Hostname# show wids whitelist ---------- White list Information ---------- Total num:1 NUM MAC-ADDRESS NAME 1 0000.0000.0001

Common Errors

N/A

1.4.2 Configuring IDS

Configuration Effect

- IDS can be used to timely find and defend against malicious or unintentional attacks in WLAN.

Notes

- IDS needs to be used together with the dynamic blacklist function, to effectively prevent attacks against WLAN.

Configuration Steps

↘ Specifying the IDS Type

- (Optional) IDS is disabled by default.
- To configure the IDS attack detection, the same as above.

Command	**attack-detection enable** { **all** | **ddos** | **flood** | **spoof** | **weak-iv** }
Parameter Description	**ddos**: Enables DDoS attack detection. **flood**: Enables flooding attack detection. **spoof**: Enables spoofing attack detection. **weak-iv**: Enables Weak IV attack detection. **all**: Enables all IDS attack detection.
Defaults	All IDS attack detection is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

↘ Configuring DDoS Attack Detection

- Optional.

- To configure the thresholds and intervals of a specified type of packets in DDoS attack detection, the same as above.

Command	**attack-detection ddos** { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }
Parameter Description	**arp-threshold** *num*: Indicates ARP packet threshold ranging from1 to 10,000 pps. **icmp-threshold** *num*: Indicates ICMP packet threshold ranging from110,000 pps. **syn-threshold** *num*: Indicates SYN packet threshold ranging from1 to 10,000 pps. **interval** *time*: Indicates the period of DDoS attack detection ranging from 10 to 60 seconds.
Defaults	By default, the interval of DDoS attack detection is 30 seconds, and the three DDoS attack detection thresholds are 50 pps for ARP packets, 100 pps for ICMP packets, and 50 pps for SYN packets.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Flooding Attack Detection

- (Optional) Flooding attack detection is disabled by default.
- To configure the threshold and interval of a specified types of packets in flooding attack detection, the same as above.
- Run the **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time* command to configure the threshold and interval of a specified type of packets for single-STA flooding attack in WIDS configuration mode.
- Run the **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time* command to configure the threshold and interval of a specified type of packets for multi-STA flooding attack in WIDS configuration mode.

Command	**attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** } **threshold** *threshold-num* **interval** *interval-time*
Parameter Description	**single-mac**: Indicates single STA detection. **total**: Indicates all packets. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *threshold-num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 5,000. *interval-time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 4,800 for multi-STA, and 10 seconds of the statistic interval
Command	WIDS configuration mode

Mode	
Usage Guide	N/A

Command	**attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time*
Parameter Description	**multi-mac**: Indicates multi-STA detection. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *threshold-num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 10,000. *interval-time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 4,800 for multi-STA, and 10 seconds of the statistic interval
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Spoofing Attack Detection

- (Optional) Spoofing attack detection is disabled by default.
- To configure the threshold and interval of a specified type of packets in spoofing attack detection, the same as above.

Command	**attack-detection spoof** { **threshold** *threshold-num* | **interval** *interval-time*}
Parameter Description	*threshold-num*: Indicates the packet threshold of spoofing attack detection ranging from 1 to 1,000. *interval-time*: Indicates the interval of spoofing attack detection ranging from 1 to 60 seconds.
Defaults	By default, the packet threshold is 1 and the detection interval is 50 seconds.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Weak IV Attack Detection

- (Optional) The Weak IV attack detection function is disabled by default.
- To configure the thresholds and intervals for specified types of packets in Weak IV attack detection, the same as above.

Command	**attack-detection weak-iv** { **threshold** *num* | **interval** *time* }
Parameter	**threshold** *num*: Indicates the packet threshold of weak IV attack detection ranging from 1 to

Description	10,000. **interval** *time*: Indicates the interval of weak IV attack detection ranging from 1 to 60 seconds.
Defaults	The default interval of Weak IV detection is 15 seconds, and the default detection threshold is 10.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Length of IDS Statistics on APs

- Optional.

Command	**attack-detection statistics ap-max** *num*
Parameter Description	*num*: Indicates the number of APs on which IDS statistics is performed. The value ranges from 1 to 1024.
Defaults	The default value is 512.
Command Mode	WIDS configuration mode
Usage Guide	N/A

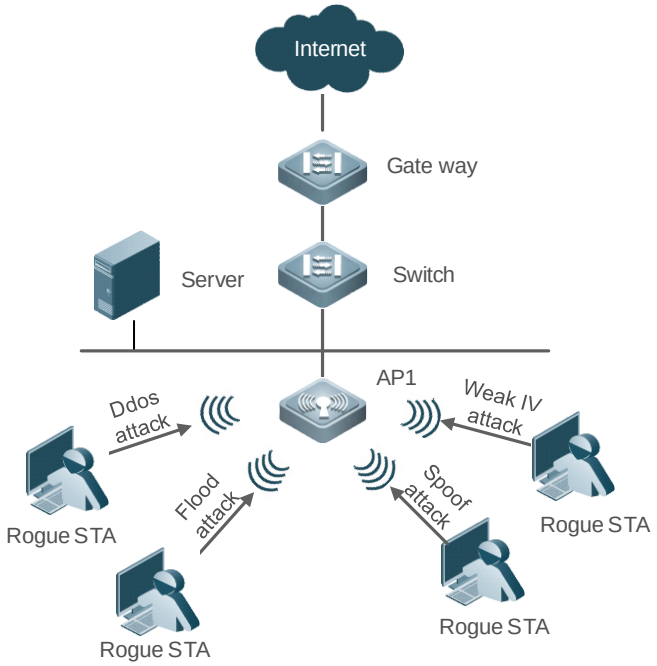
Verification

Carry out related verifications based on the IDS attack detection type:

- DDoS attack detection, detecting the ARP packet attack, ICMP packet attack and SYN packet attack.
- Flooding attack detection, detecting the multi-STA flooding attack and single-STA flooding attack.
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication packet attacks.
- Weak IV attack detection, detecting the weak IV packet attack.

Configuration Example

Configuring DDoS Attack Detection

Scenario **Figure 1-6**	
Configuration Steps	● Specify the IDS type and configure related thresholds on AP. Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# attack-detection enable flood Hostname(config-wids)# attack-detection ddos interval 10
Verification	● If a DDoS attack exists, related syslog information will be printed on AP. *Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ARP DDOS attack to Ap (1414.0902.0016). Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ICMP DDOS attack to Ap (1414.0902.0016). Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): SYN DDOS attack to Ap (1414.0902.0016).

Common Errors

N/A

1.4.3 Configuring User Isolation

Configuration Effect

- After user isolation is configured, direct communication cannot be conducted between STAs meeting the user isolation rules.

Notes

- User isolation is only valid for layer-2STAs.

Configuration Steps

Configuring the User Isolation Mode

- Optional.
- Unless otherwise noted, configure this function on ACs.

Command	**user-isolation** { **ap** | **ssid-ap** } **enable**
Parameter Description	**ap:** Indicates AP-based layer-2 user isolation. **ssid-ap:** Indicates AP-SSID-based layer-2 user isolation.
Defaults	User isolation is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Permissible MAC List for User Isolation

- Optional.
- Unless otherwise noted, configure this information on devices.
- To configure the isolation list length, the same as above.

Command	**user-isolation permit-mac** { *H.H.H* | **max** *num* }
Parameter Description	*H.H.H*: Indicates the permissible MAC list entry for user isolation. **max** *num*: Indicates the permissible MAC list length for user isolation ranging from 1 to 2,048.
Defaults	The permissible STA's MAC list for isolation is empty, with the default length of 1,024.
Command Mode	WIDS configuration mode
Usage Guide	N/A

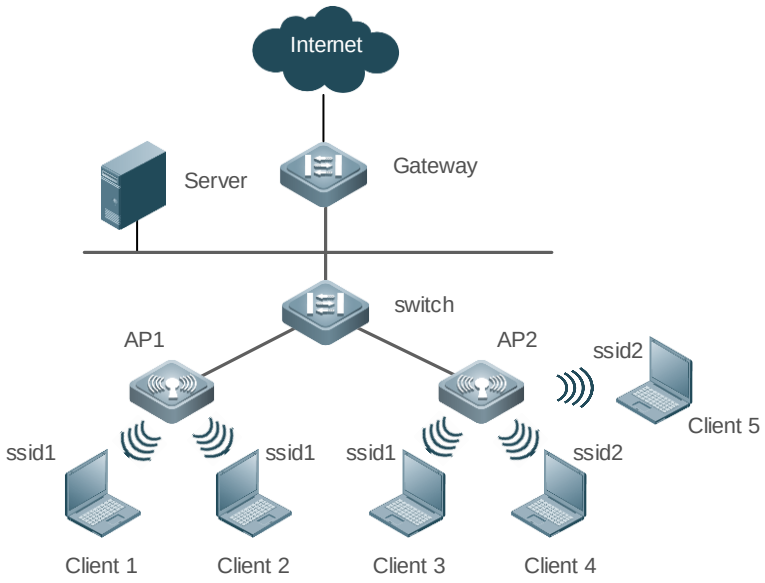
Verification

- Carry out related verifications based on the isolation mode.

Configuration Example

Configuring User Isolation

Scenario	

Figure 1-7	
Configuration Steps	● Configure the AP-based layer-2 user isolation on the AP.
	Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# user-isolation ap enable
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA.
	Hostname#show running-config ... ! wids user-isolation ap enable !

Common Errors

N/A

1.4.4 Configuring Rogue Detection and Containment

Configuration Effect

Configure Rogue detection and containment provide illegal device suppression and maintain WLAN security.

Notes

The detection and containment of Rogue devices takes effect only when the AP working mode is Hybrid or Monitor.

Configuration Steps

Enabling Rogue Containment

- Optional. Run the **countermeasures enable** command to enable Rogue containment in WIDS configuration mode.

Command	**countermeasures enable**
Parameter Description	N/A
Defaults	Rogue containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Interval

- Optional. Run the **countermeasures interval** *time* command to configure the interval of Rogue containment in WIDS configuration mode.

Command	**countermeasures interval** *time*
Parameter Description	*time*: Indicates the containment interval ranging from 100 to 10,000 ms.
Defaults	The default containment interval is 1,000 ms.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Mode

- Optional.
- Run the **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** } command to configure the Rogue containment mode in WIDS configuration mode.

Command	**countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }
Parameter Description	**adhoc**: Indicates Ad-hoc containment mode, countering Ad-hoc devices. **config**: Indicates Config containment mode, countering devices which meet entries in the SSID blacklist and static attack list. **rogue**: Indicates Rogue containment mode, countering devices whose RSSI is larger than the threshold. **ssid**: Indicates SSID containment mode, countering devices with the same SSID but not on the same device. **all**: Indicates all the above containment modes.
Defaults	No containment mode is specified by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the device operates in Normal mode.

Configuring the Static Attack List

- Optional. Run the **device attack mac-address** *H.H.H* command to configure the static attack statistic list information in WIDS configuration mode.

Command	**device attack** { **mac-address** *H.H.H* | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static attack list entry. **max** *num*: Indicates the length of the static attack list, ranging from 1 to 1,024.
Defaults	The static attack list is empty, and the length of the static attack list is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the SSID-based Blocklist

- Optional. Run the **device black-ssid** *ssid* command to configure the SSID blacklist information in WIDS configuration mode.

Command	**device** { **black-ssid** *ssid* | **max-black-ssid** *num* }
Parameter Description	**black-ssid** ssid: Indicates the SSID blacklist entry. **max-black-ssid** *num*: Indicates the SSID blacklist length, ranging from 1 to 1,024.
Defaults	The SSID blacklist is empty, and the SSID blacklist length is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Lists of Permissible MACs, SSIDs and Vendors

- Optional.
- Run the **device permit mac-address** *H.H.H* command to configure the permissible MAC list entry in WIDS configuration mode.
- Run the **device permit ssid** *H.H.H* command to configure the permissible SSID list entry in WIDS configuration mode.
- Run the **device permit vendor** *H.H.H* command to configure the permissible vendor list entry in WIDS configuration mode.

Command	**device permit** { **mac-address** *H.H.H* | **mac-address max** *num* | **ssid** *ssid* | **max-ssid** *num* | **vendor bssid** *H.H.H* | **vendor bssid max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the permissible MAC list entry, null by default. **mac-address max** *num*: Indicates the permissible MAC list length, ranging from 1 to 2,048, 1,024 by default. **ssid** *ssid*: Indicates the permissible SSID list entry, null by default. **max-ssid** *num*: Indicates the permissible SSID list length, ranging from 1 to 1,024, 512 by default. **vendor bssid** *H.H.H*: Indicates the permissible vendor list entry, null by default. **vendor bssid max** *num*: Indicates the permissible vendor list length, ranging from 1 to 1,024, 512 by default.
Defaults	N/A
Command Mode	WIDS configuration mode

Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Maximum Number of Contained Devices Once

- Optional.
- Run the **countermeasures ap-max** *ap-num* command to configure the quantity of one-time Rogue device containment in WIDS configuration mode.
- Unless otherwise noted, configure this on devices which need to configure the contained Rogue device quantity.

Command	**countermeasures ap-max** *ap-num*
Parameter Description	*ap-num*: Indicates the maximum number of countered devices each time, ranging from 1 to 256.
Defaults	The default maximum number of countered devices is 30.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Aging Duration of the Detected Devices

- Optional. Run the **device aging duration** *time* command to configure the aging duration of the detected devices in WIDS configuration mode.

Command	**device aging duration** *time*
Parameter Description	*time*: Indicates the aging duration, ranging from 500 to 5,000 seconds.
Defaults	The default aging duration is 1,200 seconds.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Device Friendly Flag

- Optional.
- Run the **device friendly-flags** *value* command to configure the device friendly flag in WIDS configuration mode. With the device friendly flag, the device can identify devices on the same device.

Command	**device friendly-flags** *value*
Parameter Description	*value*: Indicates the device friendly flag, ranging from 1 to 4294967295.
Defaults	The default value is 0.
Command Mode	WIDS configuration mode
Usage Guide	By configuring the friendly flag, AP is able to recognize a friendly AP. The default is random configuration.

Configuring the Minimum Containment RSSI

- Optional.

- Run the **countermeasures rssi-min** *num* command to configure the minimum containment RSSI in WIDS configuration mode. A Rogue device which exceeds this RSSI will be countered.

Command	**countermeasures rssi-min** *num*
Parameter Description	*num*: Indicates the minimum containment RSSI, ranging from 0 to 75 (-95 to -20).
Defaults	The default minimum containment RSSI is 25 (-70) by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Enabling Channel-Based Containment

- Optional. Run the **countermeasures channel-match** command to enable channel-based containment function in WIDS configuration mode. The channel-based containment can be conducted based on the channel on which the detected Rough device operates.

Command	**countermeasures channel-match**
Parameter Description	**N/A**
Defaults	Channel-based containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring Fuzzy Containment

- Optional.
- Run the **countermeasures fuzzy-enable** command to configure the fuzzy containment function in WIDS configuration mode. Fuzzy match is performed based on the SSID of the rogue AP. For example, if the SSID of the local host is RUIJIE-WEB, the rogue AP whose SSID is RU1JIE-WEB can be contained after the fuzzy containment function is enabled.
- Unless otherwise specified, configure the fuzzy containment function on devices which require this function.

Command	**countermeasures fuzzy-enable**
Parameter Description	N/A
Defaults	The fuzzy containment function is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	If containment modes include the configuration containment mode, rogue APs whose SSID are similar to those in the SSID blacklist are contained. If containment modes include the SSID containment mode, rogue APs whose SSIDs are similar to the SSID of the local host are contained. Fuzzy containment takes effect only in configuration containment mode and SSID containment mode.

Configuring a Fuzzy Containment Keyword

- Optional. Run the **countermeasures fuzzy-keyword** *string* command to configure a fuzzy containment keyword in WIDS configuration mode. Fuzzy containment can be performed by keyword. For example, if the configured fuzzy containment keyword is ruijie, rogue APs whose SSIDs contain ruijie such as ruijie-free can be contained after the fuzzy containment function is enabled. The keyword is case-insensitive. For example, assume that the configured fuzzy containment keyword is ruijie. There are 2^6 uppercase and lowercase combinations of ruijie. Once the fuzzy containment keyword is set to any of the combinations, APs whose SSIDs contain any combination of ruijie can be identified, such as RUIjie and RuiJie.
- Unless otherwise specified, configure a fuzzy containment keyword on devices requires this function.

Command	**countermeasures fuzzy-keyword** *string*
Parameter Description	*string*: Indicates the fuzzy containment keyword, which is case-insensitive and stored in lowercase.
Defaults	No fuzzy containment keyword is configured by default.
Command Mode	WIDS configuration mode
Usage Guide	The configuration takes effect only after the **countermeasures fuzzy-enable** command is executed. When the containment mode covers the SSID mode, rogue APs whose SSIDs contain the configured keyword will be contained. The fuzzy containment keyword takes effect only in SSID mode.

Enabling Unknown STA Detection and Containment

- Optional.
- Run the **device unknown-sta dynamic-enable** command to enable the unknown STA detection and containment function in WIDS configuration mode.
- Run the **device unknown-sta mac-address** *H.H.H* command to configure the unknown STA list entry in WIDS configuration mode.

Command	**device unknown-sta** { **dynamic-enable** | **mac-address** *H.H.H* | **mac-address max** *num* }
Parameter Description	**dynamic-enable**: Enables unknown STA detection and containment. **mac-address** *H.H.H*: Configures the unknown STA list entry, empty by default. **mac-address max** *num*: Configures the unknown STA list length, ranging from 1 to 256.
Defaults	Unknown STA detection and containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.
Command	**rogue-ap countermeasuresdevice unknown-sta report enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	The function takes effect only when the AP does not operate in Normal mode. The scanning result can be sent to the AC for display.

Configuring the Maximum Number of Detected APs

- Optional. Run the **device detected-ap-max** *num* command to configure the maximum number of detected APs in WIDS configuration mode. A smaller configuration value leads to less data being detected on the AP. If less data is detected, the device containment function may not show an obvious containment effect. A larger configuration value requires more memory.
- Unless otherwise noted, configure this on devices which need the maximum number of detected APs.

Command	**device detected-ap-max** *num*
Parameter Description	*num*: Indicates the maximum number of detected APs, ranging from 1 to 4,096.
Defaults	The default maximum number is 2,048.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Scanning Status of a Specified Radio

- Optional. Run the **hybrid-scan radio** *num* { **disable | enable** } command to configure the scanning status of a specified radio in AP configuration mode. If disabling the configuration leads to AP working in non-normal mode, there will be no device detection data.
- Unless otherwise noted, configure this on devices which need the radio scanning status.

Command	**hybrid-scan radio** *num* { **enable	disable** }
Parameter Description	*num*: Indicates a radio ID.
Defaults	All radio scanning is enabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Scanning Channel of a Specified AP

- Optional. Run the **scan-channels** { **802.11a** | **802.11b** } **channels** *num1 num2...num13* command to configure the scanning channel in AP configuration mode. If the scanning channel is not configured, there will be no device detection data when the AP operates not in Normal mode.
- Unless otherwise noted, configure this on devices which need the specified AP scanning channel.

Command	**scan-channels** { **802.11a**	**802.11b** } **channels** *num1 num2...num13*
Parameter Description	*num*: Indicates a channel number.
Defaults	The scanning channel is null.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Automatic Channel Scanning Between Different Frequency Bands

- Optional. Run the **scan-channels** { **dual-band** | **all-band** } **radio** *radio-id* command to perform automatic channel scanning among multiple frequency bands, to obtain the scanning result these frequency bands and perform containment.

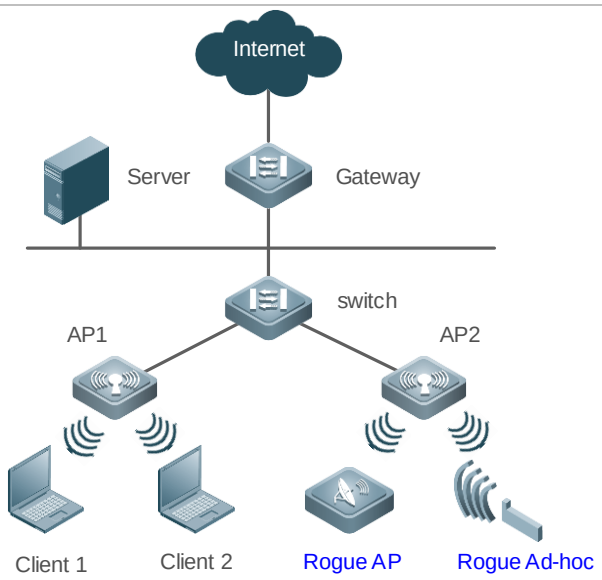
Command	**scan-channels dual-band radio** *radio-id*
Parameter Description	*radio-id*: Indicates the radio ID of the AP for which automatic channel scanning between different frequency bands is enabled.
Defaults	Automatic channel scanning between different frequency bands is disabled by default.
Command Mode	AP configuration mode
Usage Guide	The RF modules of partial APs support multiple frequency bands. When the RF modules are used for channel scanning, this command can be used for automatic channel scanning among multiple frequency bands, to obtain the scanning results of these frequency bands and perform containment. After the frequency bands are switched, channels configured by running the **scan-channels** { **802.11a**	**802.11b**	**6GHz** } **channels** command are scanned. Dual-band scans only 2.4 GHz and 5 GHz radios while all-band scans all radios supported by the AP. In addition, for some APs that have channel restrictions, the restricted channels will be automatically skipped during channel scanning.

Verification

- Run the **show wids detected** command to display the detected results.

Configuration Example

↘ Configuring Rogue Containment

Scenario	
Figure 1-8	
Configuration Steps	- Configure Rogue containment information on the device. Before configuring containment, confirm that the WLAN service has been deployed on the contained AP; otherwise, the containment will not take effect.

	Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# countermeasures enable Hostname(config-wids)# countermeasures mode ssid
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA and the log information generated by the system recently.
	Hostname#show running-config ... ! wids countermeasures enable countermeasures mode SSID ! ...

Common Errors

N/A

1.4.5 Configuring AP Working Mode

Configuration Effect

- Based on the configured working mode, the AP can provide different services.

Notes

N/A

Configuration Steps

↘ Configuring AP Working Modes

- Optional.
- Unless otherwise noted, configure this on each AP.

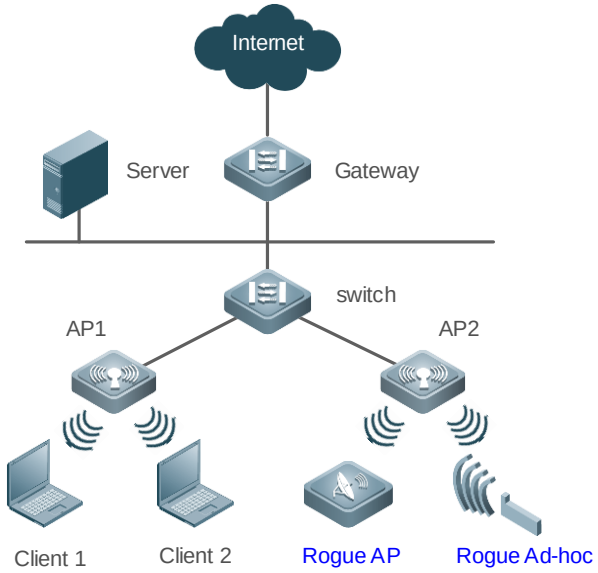
Command	**device mode** { **hybrid** | **monitor** [**radio** *radio-id*] | **normal** }
Parameter Description	**hybrid**: Indicates Hybrid mode, in which the device provides both monitoring service and access service. **monitor:** Indicates Monitor mode, in which the device provides only the monitoring service. **normal**: Indicates Normal mode, in which the device provides only the access service. *radio-id*: Specifies a radio to provide the monitoring service, while other radios to provide the access service.
Defaults	The working mode of the AP is Normal.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the current working mode of the AP.

Configuration Example

↘ Configuring the AP Working Mode

Scenario **Figure 1-9**	
Configuration Steps	• Configure the working mode of a specified AP. Hostname# configure terminal Hostname(config)# wids Hostname(config-wids)# device mode hybrid
Verification	• Run the **show running** command to display the information on related parameters configured by the STA. Hostname#show running ! wids device mode hybrid !

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the entries in the static attack list.	**reset attack-list all**
Clears the entries in the SSID-based blocklist.	**reset black-ssid all**
Clears the information of a specified device that is detected.	**reset detected { all | adhoc | rogue { ap | client } | mac-address H.H.H }**

Clears the entries in the dynamic blocklist.	**reset dynamic-blacklist { all | mac-address H.H.H }**
Clears the configuration of fuzzy containment keywords.	**reset fuzzy-keyword all**
Clears the entries in the allowed MAC list.	**reset permit-mac all**
Clears the entries in the allowed SSID list.	**reset permit-ssid all**
Clears the entries in the allowed vendor list.	**reset permit-vendor all**
Clears all or specified entries in the SSID-based blocklist and allowlist.	**reset ssid-filter { ssid all | in-ssid ssid }**
Clears all or specified entries in the SSID-based blocklist.	**reset ssid-filter { blacklist all | in-ssid ssid }**
Clears all or specified entries in the SSID-based allowlist.	**reset ssid-filter { whitelist all | in-ssid ssid }**
Clears the entries in the static blocklist.	**reset static-blacklist all**
Clears the information of the static attack statistic list.	**reset statistic all**
Clears the entries in the unknown STA list.	**reset unknown-sta all**
Clears the entries in the allowed list for user isolation.	**reset user-isolation-permit-list all**
Clears the entries in the allowlist.	**reset whitelist all**

Displaying

Description	Command
Displays the configuration of the attack list.	**show wids attack-list**
Displays the configuration of the dynamic and static blocklists.	**show wids blacklist** { **dynamic** | **static** }
Displays the configuration of the SSID-based blocklist.	**show wids black-ssid**
Displays the information of a specified device that is detected.	**show wids detected** { **adhoc** | **all** | **friendly ap** | **interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }

Configuring Wireless Authentication

1. Configuring AAA
2. Configuring RADIUS
3. Configuring IEEE 802.1X
4. Configuring Web Authentication
5. Configuring SCC

1 Configuring AAA

1.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring the authentication, authorization, and accounting services. Devices support the AAA application.

AAA provides the following services in a modular way:

Authentication: Refers to the verification of user identities for network access and network services. Authentication is classified into local authentication and authentication through Remote Authentication Dial In User Service (RADIUS).

Authorization: Refers to the granting of specific network services to users according to a series of defined attribute-value (AV) pairs. The pairs describe what operations users are authorized to perform. AV pairs are stored on network access servers (NASs) or remote authentication servers.

Accounting: Refers to the tracking of the resource consumption of users. When accounting is enabled, NASs collect statistics on the network resource usage of users and send them in AV pairs to authentication servers. The records will be stored on authentication servers, and can be read and analyzed by dedicated software to realize the accounting, statistics, and tracking of network resource usage.

AAA is the most fundamental method of access control. Devices also 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.
Configuring AAA in a Multi-Domain Environment	AAA is performed for the users in different domains by using different methods.

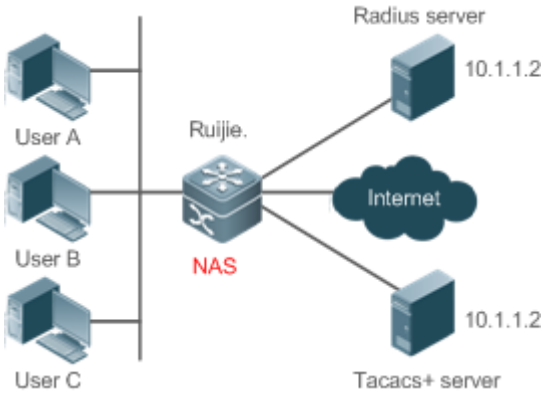
1.2.1 Configuring AAA in a Single-Domain Environment

Scenario

In the network scenario shown in Figure 1-1, the following application requirements must be satisfied to improve the security management on the NAS:

1. To facilitate account management and avoid information disclosure, each administrator has an individual account with different username and password.
2. Users must pass identity authentication before accessing the NAS. The authentication can be in local or centralized mode. It is recommended to combine the two modes, with centralized mode as active and local mode as standby. As a result, users must undergo authentication by the RADIUS server first. If the RADIUS server does not respond, it turns to local authentication.
3. During the authentication process, users can be classified and limited to access different NASs.
4. Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
5. The AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 1-1



Remarks	User A, User B, and User C are connected to the NAS in wired or wireless way. The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure the authentication service on the NAS.
- Configure the authorization service on the NAS.
- Configure the accounting service on the NAS.

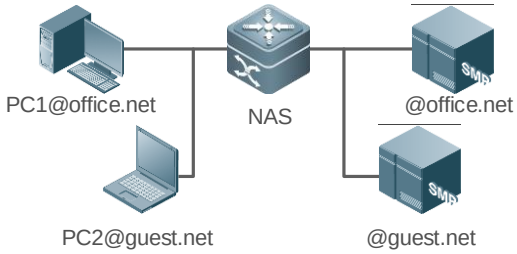
1.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@office.net or PC2@guest.net and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
- The AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 1-2



Remarks	The clients with the usernames **PC1@office.net** and **PC2@guest.net** are connected to the NAS in wired or wireless way. The NAS is an access switch. The Security Accounts Manager (SAM) server is a universal RADIUS server provided by Ruijie Networks.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Define an AAA method list on the NAS.
- Enable domain-based AAA on the NAS.
- Create domains and AV sets on the NAS.

1.3 Features

Basic Concepts

↘ Local Authentication and Remote Server Authentication

Local authentication is the process where the entered passwords are verified by the database on the NAS.

Remote server authentication is the process where the entered passwords are checked by the database on a remote server. It is mainly implemented by the RADIUS server.

↘ 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 devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 1-3

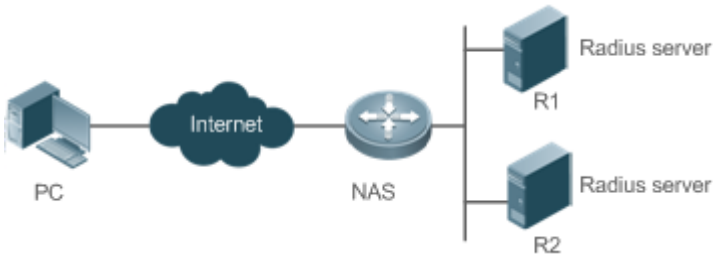


Figure 1-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

Assume that the system administrator defines a method list, where the NAS selects R1 and R2 in sequence to obtain user identity information and then accesses the local username database on the server. For example, when a remote PC user initiates dial-up access, the NAS first queries the user's identity on R1. When the authentication on R1 is completed, R1 returns an Accept response to the NAS. Then the user is permitted to access the Internet. If R1 returns a Reject response, the user is denied Internet access and the connection is terminated. If R1 does not respond, the NAS considers that the R1 method times out and continues to query the user's identity on R2. This process continues as the NAS keeps trying the remaining authentication methods, until the user request is authenticated, rejected, or terminated. If all the authentication methods are responded with Timeout, authentication fails and the connection will be terminated.

ℹ 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.

ℹ This document describes how to configure AAA on the RADIUS server.

AAA Server Group

You can define an AAA server group to include one or more servers of the same type. If the server group is referenced by a method list, the NAS preferentially sends requests to the servers in the referenced server group when the method list is used to implement AAA.

Overview

Feature	Description
AAA Authentication	Verifies whether users can access the Internet.
AAA Authorization	Determines what services or permissions users can enjoy.
AAA Accounting	Records the network resource usage of users.
Multi-Domain AAA	Creates domain-specific AAA schemes for stations (STAs) in different domains.

1.3.1 AAA Authentication

Authentication, authorization, and accounting are three independent services. The authentication service verifies whether users can access the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can use only the authentication service of AAA.

To configure AAA authentication, you need to first configure an authentication method list. Applications perform authentication according to the method list. The method list defines the types of authentication and the sequence in which they are performed. Authentication methods are implemented by specified applications. The only exception is the default method list. All applications use the default method list if no method list is configured.

AAA Authentication Scheme

- No authentication (**none**)

The identity of trusted users is not checked. Normally, the no-authentication (None) method is not used.

- Local authentication (**local**)

Authentication is performed on the NAS, which is configured with user information (including usernames, passwords, and AV pairs). Before local authentication is enabled, run the **username password/secret** command to create a local user database.

- Remote server group authentication (**group**)

Authentication is performed jointly by the NAS and a remote server group through RADIUS. 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).

- Point-to-Point Protocol (PPP) authentication

PPP authentication is performed for users that initiate dial-up access through PPP.

- Dot1X (IEEE802.1X) authentication

Dot1X (IEEE802.1X) authentication is performed for users that initiate dial-up access through IEEE802.1X.

- iPortal (built-in portal) authentication

iPortal authentication is performed by the first generation portal server.

- Web (second generation Portal) authentication

Web authentication is performed by the second generation Portal server.

- General authentication

Specify a general authentication method for 802.1X authentication, built-in Portal authentication, and the second generation Portal authentication.

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 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 server in advance. If local authorization needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Authorization Method List

By default, no AAA authorization method list is configured.

Determine the access mode to be configured in advance. Then configure authorization methods according to the access mode.

1.3.3 AAA Accounting

In AAA, accounting is an independent process of the same level as authentication and authorization. During the accounting process, start-accounting, update-accounting, and end-accounting requests are sent to the configured accounting server, which records the network resource usage of users and performs accounting, audit, and tracking of users' activities.

In AAA configuration, accounting scheme configuration is optional.

AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

Accounting is completed on the NAS, which collects statistics on and limits the number of local user connections. Billing is not performed.

- Remote server-group accounting (**group**)

Accounting is performed jointly by the NAS and a remote server group. You can configure local accounting as standby to avoid accounting failures when all the servers in the server group fail.

AAA Accounting Types

- EXEC accounting

Accounting is performed when users log in to and out of the CLI of the NAS.

- Command accounting

Records are kept on the commands that users run on the CLI of the NAS.

- Network accounting

Records are kept on the sessions that users set up after completing 802.1X and Web authentication to access the Internet.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Accounting Scheme

By default, no AAA accounting method is configured.

Before you configure an AAA accounting scheme, determine whether to use local accounting or remote server-group accounting. If remote server-group accounting needs to be implemented, configure a RADIUS server in advance. If local accounting needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Accounting Method List

By default, no AAA accounting method list is configured.

Determine the access mode to be configured in advance. Then configure accounting methods according to the access mode.

1.3.4 Multi-Domain AAA

In a multi-domain environment, the NAS can provide the AAA services to users in different domains. The user AVs (such as usernames and passwords, service types, and permissions) may vary with different domains. It is necessary to configure domains to differentiate the user AVs in different domains and configure an AV set (including an AAA service method list, for example, RADIUS) for each domain.

Our products support the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

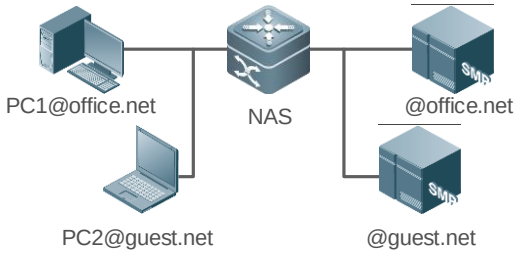
The fourth format (userid) does not contain a domain name, and it is considered to use the **default** domain name.

The NAS provides the domain-based AAA service based on the following principles:

- Resolves the domain name carried by a user.
- Searches for the user domain according to the domain name.
- Searches for the corresponding AAA method list name according to the domain configuration information on the NAS.
- Searches for the corresponding method list according to the method list name.
- Provides the AAA services based on the method list.

If any of the preceding procedures fails, the AAA services cannot be provided.

Figure 1-4 shows the typical multi-domain topology.



Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Method List

By default, no AAA method list is configured.

Enabling the Domain-Based AAA Service

By default, the domain-based AAA service is disabled.

To enable the domain-based AAA service, run the **aaa domain enable** command.

Creating a Domain

By default, no domain is configured.

To configure a domain, run the **aaa domain** *domain-name* command.

Configuring an AV Set for a Domain

By default, no domain AV set is configured.

A domain AV set contains the following elements: AAA method lists, the maximum number of online users, whether to remove the domain name from the username, and whether the domain name takes effect.

Displaying Domain Configuration

To display domain configuration, run the **show aaa domain** command.

The system supports a maximum of 32 domains.

1.4 Configuration

Configuration	Description and Command	
Configuring AAA Authentication	Mandatory if user identities need to be verified.	
	aaa new-model	Enables AAA.
	aaa authentication login	Defines a method list of login authentication.
	aaa authentication enable	Defines a method list of Enable authentication.
	aaa authentication dot1x	Defines a method list of 802.1X authentication.
	aaa authentication ppp	Defines a method list of PPP authentication.
	aaa authentication sslvpn	Defines a method list of SSL VPN authentication.
	aaa authentication web-auth	Defines a method list of Web authentication.
	aaa authentication iportal	Defines a method list of built-in Portal authentication.
	aaa authentication general	Defines a method list of general authentication.

Configuration	Description and Command	
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the maximum lockout time after a login failure.
Configuring AAA Authorization	⚠ Mandatory if different permissions and services need to be assigned to users.	
	aaa new-model	Enables AAA.
	aaa authorization exec	Defines a method list of EXEC authorization.
	aaa authorization network	Configures a method list of network authorization.
	authorization exec	Applies EXEC authorization methods to a specified VTY line.
	authorization commands	Applies command authorization methods to a specified VTY line.
Configuring AAA Accounting	⚠ Mandatory if accounting, statistics, and tracking need to be performed on the network resource usage of users.	
	aaa new-model	Enables AAA.
	aaa accounting exec	Defines a method list of EXEC accounting.
	aaa accounting commands	Defines a method list of command accounting.
	aaa accounting network	Defines a method list of network accounting.
	accounting exec	Applies EXEC accounting methods to a specified VTY line.
	aaa accounting update	Enables accounting update.
	aaa accounting update periodic	Configures the accounting update interval.
Configuring an AAA Server Group	⚠ Recommended if a server group needs to be configured to handle AAA through different servers in the group.	
	aaa group server	Creates a user-defined AAA server group.
	server	Adds an AAA server group member.
Configuring Domain-Based AAA Service	⚠ Mandatory if AAA management of 802.1X access STAs needs to be performed according to domains.	
	aaa new-model	Enables AAA.
	aaa domain enable	Enables the domain-based AAA service.
	aaa domain	Creates a domain and enters domain configuration mode.
	authentication dot1x	Associates the domain with an 802.1X authentication method list.

Configuration	Description and Command	
	accounting network	Associates the domain with a network accounting method list.
	authorization network	Associates the domain with a network authorization method list.
	state	Configures the domain status.
	username-format	Configures whether to contain the domain name in usernames.
	access-limit	Configures the maximum number of domain users.
Configuring a Policy for Accounting-Start Failures	**aaa accounting start-fail**	Configures a policy for accounting-start failures.
Configuring Heartbeat Packet Detection	[**no**] **aaa heartbeat enable**	Configures heartbeat detection.
Configuring AAA Logging	[**no**] **aaa log enable**	Configures AAA logging.
	aaa log rate-limit *num*	Configures an 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.

Normally, do not use None authentication. You can use the **none** method as the last optional authentication method in special cases. For example, all the users who may request access are trusted users and the users' work must not be delayed by system faults. Then you can use the **none** method to assign access permissions to these users when the authentication server does not respond. It is recommended that the local authentication method be added before the **none** method.

- If AAA authentication is enabled but no authentication method is configured and the default authentication method does not exist, users can directly log in to the Console without being authenticated. If users log in by other means, the users must pass local authentication.
- When a user enters the CLI after passing login authentication (the **none** method is not used), the username is recorded. When the user performs Enable authentication, the user is not prompted to enter the username again, because the username that the user entered during login authentication is automatically filled in. However, the user must enter the password previously used for login authentication.

- The username is not recorded if the user does not perform login authentication when entering the CLI or the **none** method is used during login authentication. Then, a user is required to enter the username each time when performing Enable authentication.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of Login Authentication

- Run the **aaa authentication login** command to configure a method list of login authentication.
- This configuration is mandatory if you need to configure a login authentication method list (including the configuration of the default method list).
- By default, no method list of login authentication is configured.

Defining a Method List of Enable Authentication

- Run the **aaa authentication enable** command to configure a method list of Enable authentication.
- This configuration is mandatory if you need to configure an Enable authentication method list. (You can configure only the default method list.)
- By default, no method list of Enable authentication is configured.

Defining a Method List of 802.1X Authentication

- Run the **aaa authentication dot1x** command to configure a method list of 802.1X authentication.
- This configuration is mandatory if you need to configure an 802.1X authentication method list (including the configuration of the default method list).
- By default, no method list of 802.1X authentication is configured.

Defining a Method List of PPP Authentication

- Run the **aaa authentication ppp** command to configure a method list of PPP authentication.
- This configuration is mandatory if you need to configure an authentication method list for PPP dial-up access.
- By default, no method list of PPP authentication is configured.

Defining a Method List of Web Authentication

- Run the **aaa authentication web-auth** command to configure a method list of Web authentication.
- This configuration is mandatory if you need to configure a Web authentication method list (including the configuration of the default method list).
- By default, no method list of Web authentication is configured.

Defining a Method List of iPortal Web Authentication

- Run the **aaa authentication iportal** command to configure a method list of iPortal Web authentication.
- This configuration is mandatory if you need to configure an iPortal Web authentication method list (including the configuration of the default method list).
- By default, no method list of iPortal Web authentication is configured.

Defining a General Method List of 802.1X Authentication, Built-in Portal authentication, and Second Generation Portal Authentication

- Run the **aaa authentication general** command to configure a method list for 802.1X authentication, built-in Portal authentication, and the second generation Portal authentication.
- If the **aaa authentication dot1x**, **aaa authentication web-auth** or **aaa authentication iportal** command is also configured, it prevails over the **aaa authentication general** command.
- By default, no general authentication method list is configured.

Defining a Method List of SSL VPN Authentication

- Run the **aaa authentication sslvpn** command to configure a method list of SSL VPN authentication.
- This configuration is mandatory if you need to configure an SSL VPN authentication method list (including the configuration of the default method list).
- By default, no method list of SSL VPN authentication is configured.

Setting the Maximum Number of Login Attempts

- Optional.
- By default, a user is allowed to enter passwords up to three times during login.

Setting the Maximum Lockout Time After a Login Failure

- Optional.
- By default, a user is locked for 15 minutes after entering wrong passwords three times.

Verification

- Run the **show aaa method-list** command to display the configured method lists.
- Run the **show aaa lockout** command to display the settings of the maximum number of login attempts and the maximum lockout time after a login failure.
- Run the **show running-config** command to display the authentication method lists associated with login authentication and 802.1X authentication.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of Login Authentication

Command	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default:** With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a login authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server groups are supported. **subs**: Indicates that the subs database is used for authentication.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform login authentication negotiation through AAA. Run the **aaa authentication login** command to configure the default or optional method lists for login authentication. In a method list, the next method is executed only when the current method does not receive response. After you configure login authentication methods, apply the methods to the VTY lines that require login authentication; otherwise, the methods will not take effect.

Defining a Method List of Enable Authentication

Command	**aaa authentication enable default** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an Enable authentication method list in characters. *method*: Indicates authentication methods from **enable**, **local**, **none**, and **group**. A method list contains up to four methods. **enable**: Indicates that the password that is configured using the **enable** command is used for authentication. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server groups are supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform Enable authentication negotiation through AAA. Run the **aaa authentication enable** command to configure the default or optional method lists for Enable authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of 802.1X Authentication

Command	**aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an 802.1X authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server group is supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA 802.1X authentication service is enabled on the NAS, users must perform 802.1X authentication negotiation through AAA. Run the **aaa authentication dot1x** command to configure the default or optional method lists for 802.1X authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of PPP, Web, iPortal or SSL VPN Authentication

Command	**aaa authentication** { **ppp | web-auth** | **iportal** | **sslvpn** } { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**ppp:** Configures a method list of PPP authentication. **web-auth**: Configures a method list of Web authentication. **iportal**: Configures a method list of iportal authentication. **sslvpn**: Configures a method list of SSL VPN authentication. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a PPP authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server groups is supported. **subs**: Specifies the SUBS authentication method using the SUBS database.
Command Mode	Global configuration mode
Usage Guide	If the AAA PPP authentication service is enabled on the NAS, users must perform PPP authentication negotiation through AAA. Run the **aaa authentication ppp** command to configure the default or optional method lists for PPP authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a General Method List of 802.1X Authentication, Built-in Portal Authentication, and Second Generation Portal Authentication

Command	**aaa authentication general** { **default** | *list-name* } *method1* [*method2*...]

Parameter Description	**default**: Indicates that the defined method list applies to all front-end authentication. *list-name*: Indicates the name of a general authentication list in characters. *method*: Indicates keyword **local**, **none**, or **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server group is supported.
Command Mode	Global configuration mode
Usage Guide	The general method list applies to only front-end services of 802.1X authentication, built-in Portal authentication, and second generation Portal authentication. If there is no response to method 1, method 2 will take effect.

Setting the Maximum Number of Login Attempts

Command	**aaa local authentication attempts** *max-attempts*
Parameter Description	*max-attempts*: Indicates the maximum number of login attempts. The value ranges from 1 to 2,147,483,647.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum number of times a user can attempt to login.

Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local authentication lockout-time** *lockout-time*
Parameter Description	*lockout-time*: Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 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 1-5	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be

	implemented. (This example requires the configuration of a RADIUS server and local database information.) Step 3: Configure an AAA authentication method list for login authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key radius-key Hostname(config)#aaa authentication login list1 group radius local Hostname(config)#line vty 0 20 Hostname(config-line)#login authentication list1 Hostname(config-line)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login list1 group radius local Accounting method-list: Authorization method-list:
	Assume that a user remotely logs in to the NAS through Telnet. The user is prompted to enter the username and password on the CLI. The user must enter the correct username and password to access the NAS.
User	User Access Verification Username:user Password:pass

↘ Configuring AAA Enable Authentication

Configure an Enable authentication method list on the NAS containing **group** *radius*, **local**, and then **enable** methods in order.

Scenario Figure 1-6	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication. Step 3: Configure an AAA authentication method list for Enable authentication users. You can define only one Enable authentication method list globally. You do not need to define the list name but just default it. After that, it will be applied automatically.
NAS	Hostname#configure terminal Hostname(config)#username user privilege 15 password pass Hostname(config)#enable secret w Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key radius-key Hostname(config)#aaa authentication enable default group radius local enable
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication enable default group radius local enable Accounting method-list: Authorization method-list:
	The CLI displays an authentication prompt when the user level is updated to level 15. The user must enter the correct username and password to access the NAS.
NAS	Hostname>enable Username:user Password:pass

	Hostname#

Configuring AAA 802.1X Authentication

Configure an 802.1X authentication method list on the NAS containing **group** *radius*, and then **local** methods in order.

Scenario **Figure 1-7**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the AAA authentication method list. Skip this step if the default authentication method is used. Step 5: Enable 802.1X authentication on an interface.
NAS	Hostname#configure terminal Hostname(config)#username user1 password pass1 Hostname(config)#username user2 password pass2 Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key radius-key Hostname(config)#aaa authentication dot1x default group radius local Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)#dot1 port-control auto Hostname(config-if-gigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication dot1x default group radius local

	Accounting method-list: Authorization method-list:

Common Errors

- RADIUS 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.
- Console authorization: The device can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Steps

↘ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

↘ Defining a Method List of EXEC Authorization

- Run the **aaa authorization exec** command to configure a method list of EXEC authorization.
- This configuration is mandatory if you need to configure an EXEC authorization method list (including the configuration of the default method list).
- By default, no EXEC authorization method list is configured.

The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)

Defining a Method List of Command Authorization

- Run the **aaa authorization commands** command to configure a method list of command authorization.
- This configuration is mandatory if you need to configure a command authorization method list (including the configuration of the default method list).
- By default, no command authorization method list is configured.

Configuring a Method List of Network Authorization

- Run the **aaa authorization network** command to configure a method list of network authorization.
- This configuration is mandatory if you need to configure a network authorization method list (including the configuration of the default method list).
- By default, no authorization method is configured.

Applying EXEC Authorization Methods to a Specified VTY Line

- Run the **authorization exec** command in line configuration mode to apply EXEC authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Applying Command Authorization Methods to a Specified VTY Line

- Run the **authorization commands** command in line configuration mode to apply command authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Enabling Authorization for Commands in Configuration Modes

- Run the **aaa authorization config-commands** command to enable authorization for commands in configuration modes.
- By default, authorization is disabled for commands in configuration modes.

Enabling Authorization for the Console to Run Commands

- Run the **aaa authorization console** command to enable authorization for console users to run commands.
- By default, authorization is disabled for the Console to run commands.

Verification

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

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Authorization

Command	**aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC authorization method list in characters. *method*: Specifies authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for EXEC authorization. **none**: Indicates that EXEC authorization is not performed. **group**: Indicates that a server group is used for EXEC authorization. Currently, the RADIUS server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The device supports authorization of the users who log in to the CLI of the NAS to assign the users CLI operation permission levels (0 to 15). Currently, EXEC authorization is performed only on the users who have passed login authentication. If a user fails in EXEC authorization, the user cannot enter the CLI. After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.

Defining a Method List of Command Authorization

Command	**aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command authorization is not performed. **group**: Indicates that a server group is used for command authorization.
Command Mode	Global configuration mode
Usage Guide	The device supports authorization of the commands executable by users. When a user enters a command, AAA sends the command to the authentication server. If the authentication server permits the execution, the command is executed. If the authentication server forbids the execution, the command is not executed and a message is displayed showing that the execution is rejected.

	When you configure command authorization, specify the command level, which is used as the default level. (For example, if a command above Level 14 is visible to users, the default level of the command is 14.) After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.

Configuring a Method List of Network Authorization

Command	**aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for network authorization.
Command Mode	Global configuration mode
Usage Guide	The device supports authorization of network-related service requests such as PPP and SLIP requests. After authorization is configured, all authenticated users or interfaces are authorized automatically. You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried. RADIUS servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.

Enabling Authorization for Commands in Configuration Modes (Including the Global Configuration Mode and Sub-Modes)

Command	**aaa authorization config-commands**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If you need to enable authorization for commands only in non-configuration modes (for example, privileged EXEC mode), disable authorization in configuration modes by using the **no** form of this command. Then users can run commands in configuration mode and sub-modes without authorization.

Enabling Authorization for the Console to Run Commands

Command	**aaa authorization console**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	The device can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Example

↘ Configuring AAA EXEC Authorization

Configure login authentication and EXEC authorization for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC authorization is performed on a RADIUS server. If the RADIUS server does not respond, users are redirected to the local authorization.

Scenario Figure 1-8	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used. EXEC authorization is often used with login authentication, which can be implemented on the same line.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#username user privilege 6 Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication login list1 group local Hostname(config)#aaa authorization exec list2 group radius local Hostname(config)#line vty 0 4 Hostname(config-line)#login authentication list1 Hostname(config-line)# authorization exec list2 Hostname(config-line)#exit

Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: Authorization method-list: aaa authorization exec list2 group radius local
	Hostname# show running-config aaa new-model ! aaa authorization exec list2 group local aaa authentication login list1 group radius local ! username user password pass username user privilege 6 ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 authorization exec list2 login authentication list1 ! End

Configuring AAA Network Authorization

Scenario **Figure 1-9**	

Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	Hostname#configure terminal Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authorization network default group radius none Hostname(config)# end
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none

Common Errors

N/A

1.4.3 Configuring AAA Accounting

Configuration Effect

- Record the network resource usage of users.
- Record the user login and logout processes and the commands executed by users during device management.

Notes

About accounting methods:

- If an accounting scheme contains multiple accounting methods, these methods are executed according to the method configuration sequence. The next accounting method is executed only when the current method does not receive response. If accounting fails using a method, the next method will be not tried.
- After the default accounting method list is configured, it is applied to all VTY lines automatically. If a non-default accounting method list is applied to a line, it will replace the default one. If you apply an undefined method list to a line, the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

- EXEC accounting is performed only when login authentication on the NAS is completed. EXEC accounting is not performed if login authentication is not configured or the **none** method is used for authentication. If Start accounting is not performed for a user upon login, Stop accounting will not be performed when the user logs out.

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.

Defining a Method List of Network Accounting

- Run the **aaa accounting network** command to configure a method list of network accounting.
- This configuration is mandatory if you need to configure a network accounting method list (including the configuration of the default method list).
- By default, no network accounting method list is configured.

Applying EXEC Accounting Methods to a Specified VTY Line

- Run the **accounting exec** command in line configuration mode to apply EXEC accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying Command Accounting Methods to a Specified VTY Line

- Run the **accounting commands** command in line configuration mode to apply command accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying 802.1X Network Accounting Methods

- Run the **dot1x accounting network** command to configure 802.1X network accounting methods.
- This configuration is mandatory if you need to specify 802.1X network accounting methods.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Enabling Accounting Update

- Optional.
- It is recommended that accounting update be configured for improved accounting accuracy.
- By default, accounting update is disabled.

Configuring the Accounting Update Interval

- Optional.
- It is recommended that the accounting update interval not be configured unless otherwise specified.

Verification

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

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Accounting

Command	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that EXEC accounting is not performed. **group**: Indicates that a server group is used for EXEC accounting. Currently, the RADIUS server groups is supported.
Command Mode	Global configuration mode
Usage Guide	The device enables EXEC accounting only when login authentication is completed. EXEC accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, when a user logs in to the CLI of the NAS, the NAS sends a start-accounting message to the authentication server. When the user logs out, the NAS sends a stop-accounting message to the authentication server. If the NAS does not send a start-accounting message when the user logs in, the NAS will not send a stop-accounting message when the user logs out. After you configure EXEC accounting methods, apply the methods to the VTY lines that require EXEC accounting; otherwise, the methods will not take effect.

Defining a Method List of Command Accounting

Command	**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*level*: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15. After a command of the configured level is executed, the accounting server records related information based on the received accounting packet. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command accounting is not performed. **group**: Indicates that a server group is used for command accounting.
Command Mode	Global configuration mode
Usage Guide	The device enables command accounting only when login authentication is completed. Command accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, the NAS records information about the commands of the configured level that users run and sends the information to the authentication server. After you configure command accounting methods, apply the methods to the VTY lines that require command accounting; otherwise, the methods will not take effect.

Defining a Method List of Network Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network accounting method list in characters. **start-stop**: Indicates that a start-accounting message and a stop-accounting message are sent when a user accesses a network and when the user disconnects from the network respectively. The start-accounting message indicates that the user is allowed to access the network, regardless of whether accounting is successfully enabled. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that network accounting is not performed. **group**: Indicates that a server group is used for network accounting. Currently, the RADIUS groups is supported.
Command Mode	Global configuration mode
Usage Guide	The device sends record attributes to the authentication server to perform accounting of user activities. The **start-stop** keyword is used to configure user accounting options.

Enabling Accounting Update

Command	**aaa accounting update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to enable accounting update.

Configuring the Accounting Update Interval

Command	**aaa accounting update periodic** *interval*
Parameter Description	*Interval*: Indicates the accounting update interval in minutes. The value ranges from 1 to 525,600.
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 1-10	

Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication login list1 group local Hostname(config)#aaa accounting exec list3 start-stop group radius Hostname(config)#line vty 0 4 Hostname(config-line)#login authentication list1 Hostname(config-line)# accounting exec list3 Hostname(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: aaa accounting exec list3 start-stop group radius Authorization method-list:
	Hostname# show running-config aaa new-model ! aaa accounting exec list3 start-stop group radius aaa authentication login list1 group local !

	username user password pass ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 accounting exec list3 login authentication list1 ! End

Configuring AAA Network Accounting

Configure a network accounting method list for 802.1X STAs, and configure a RADIUS remote server for authentication and accounting.

Scenario Figure 1-11	
Configuration Steps	Step 1: Enable AAA. Step 2: If remote server-group accounting needs to be implemented, configure a RADIUS server in advance. Step 3: Configure an AAA accounting method list according to different access modes and service types. Step 4: Apply the configured AAA accounting method list. Skip this step if the default accounting method is used. Accounting is performed only when 802.1X authentication is completed.
NAS	Hostname#configure terminal Hostname(config)#username user password pass Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication dot1x aut1x group radius local Hostname(config)#aaa accounting network acc1x start-stop group radius

	Hostname(config)#dot1x authentication aut1x Hostname(config)#dot1x accounting acc1x Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#dot1 port-control auto Hostname(config-if-GigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication dot1x aut1x group radius local Accounting method-list: aaa accounting network acc1x start-stop group radius Authorization method-list:

Common Errors

N/A

1.4.4 Configuring an AAA Server Group

Configuration Effect

- Create a user-defined server group and add one or more servers to the group.
- When you configure authentication, authorization, and accounting method lists, name the methods after the server group name so that the servers in the group are used to handle authentication, authorization, and accounting requests.
- Use self-defined server groups to separate authentication, authorization, and accounting.

Notes

In a user-defined server group, you can specify and apply only the servers in the default server group.

Configuration Steps

↘ Creating a User-Defined AAA Server Group

- Mandatory.
- Assign a meaningful name to the user-defined server group. Do not use the predefined **radius** keywords in naming.

↘ Adding an AAA Server Group Member

- Mandatory.

- Run the **server** command to add AAA server group members.
- By default, a user-defined server group does not have servers.

Verification

Run the **show aaa group** command to verify the configuration.

Related Commands

Creating a User-Defined AAA Server Group

Command	**aaa group server radius** *name*
Parameter Description	*name*: Indicates the name of the server group to be created. The name must not contain the **radius** keywords because they are the names of the default RADIUS server groups.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an AAA server group. Currently, the RADIUS server groups is supported.

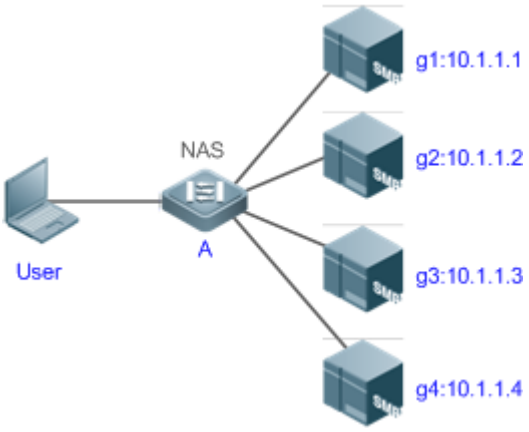
Adding an AAA Server Group Member

Command	**server** *ipv4-addr* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ipv4-addr*: Indicates the IP address of a server. *port1*: Indicates the authentication port of a server. (This parameter is supported only by the RADIUS server group.) *port2*: Indicates the accounting port of a server. (This parameter is supported only by the RADIUS server group.)
Command Mode	Server group configuration mode
Usage Guide	When you add servers to a server group, the default ports are used if you do not specify ports.

Configuration Example

Creating an AAA Server Group

Create RADIUS server groups named g1 and g2. The IP addresses of the servers in g1 are 10.1.1.1 and 10.1.1.2, and the IP addresses of the servers in g2 are 10.1.1.3 and 10.1.1.4.

Scenario **Figure 1-12**	
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable. 2. Enable AAA.
Configuration Steps	Step 1: Configure a server (which belongs to the default server group). Step 2: Create user-defined AAA server groups. Step 3: Add servers to the AAA server groups.
NAS	Hostname#configure terminal Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server host 10.1.1.2 Hostname(config)#radius-server host 10.1.1.3 Hostname(config)#radius-server host 10.1.1.4 Hostname(config)#radius-server key secret Hostname(config)#aaa group server radius g1 Hostname(config-gs-radius)#server 10.1.1.1 Hostname(config-gs-radius)#server 10.1.1.2 Hostname(config-gs-radius)#exit Hostname(config)#aaa group server radius g2 Hostname(config-gs-radius)#server 10.1.1.3 Hostname(config-gs-radius)#server 10.1.1.4 Hostname(config-gs-radius)#exit
Verification	Run the **show aaa group** and **show run** commands on the NAS to display the configuration.
NAS	Hostname#show aaa group

	Type Reference Name ---------- ---------- ---------- radius 1 radius radius 1 g1 radius 1 g2
	Hostname#show run ! radius-server host 10.1.1.1 radius-server host 10.1.1.2 radius-server host 10.1.1.3 radius-server host 10.1.1.4 radius-server key secret ! aaa group server radius g1 server 10.1.1.1 server 10.1.1.2 ! aaa group server radius g2 server 10.1.1.3 server 10.1.1.4 ! !

Common Errors

- For RADIUS servers that use non-default authentication and accounting ports, when you run the **server** command to add servers, specify the authentication or accounting port.

1.4.5 Configuring Domain-Based AAA Service

Configuration Effect

Create AAA schemes for 802.1X users in different domains.

Notes

About referencing method lists in domains:

- The AAA method lists that you select in domain configuration mode should be defined in advance. If the method lists are not defined in advance, when you select them in domain configuration mode, the system prompts that the configurations do not exist.
- The names of the AAA method lists selected in domain configuration mode must be consistent with those of the method lists defined for the AAA service. If they are inconsistent, the AAA service cannot be properly provided to the users in the domain.

About the default domain:

- Default domain: After the domain-based AAA service is enabled, if a username does not carry domain information, the AAA service is provided to the user based on the default domain. If the domain information carried by the username is not configured in the system, the system determines that the user is unauthorized and will not provide the AAA service to the user. If the default domain is not configured initially, it must be created manually.
- When the domain-based AAA service is enabled, the default domain is not configured by default and needs to be created manually. The default domain name is **default**. It is used to provide the AAA service to the users whose usernames do not carry domain information. If the default domain is not configured, the AAA service is not available for the users whose usernames do not carry domain information.

About domain names:

- The domain names carried by usernames and those configured on the NAS are matched in the longest matching principle. For example, if two domains, **domain.com** and **domain.com.cn** are configured on a NAS and a user sends a request carrying **aaa@domain.com**, the NAS determines that the user belongs to **domain.com**, instead of **domain.com.cn**.
- If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the AAA service is not provided to the user.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Enabling the Domain-Based AAA Service

- Mandatory.
- Run the **aaa domain enable** command to enable the domain-based AAA service.
- By default, the domain-based AAA service is disabled.

Creating a Domain and Entering Domain Configuration Mode

- Mandatory.
- Run the **aaa domain** command to create a domain or enter the configured domain.
- By default, no domain is configured.

Associating the Domain with an 802.1X Authentication Method List

- Run the **authentication dot1x** command to associate the domain with an 802.1X authentication method list.
- This configuration is mandatory if you need to apply a specified 802.1X authentication method list to the domain.
- Currently, the domain-based AAA service is applicable only to 802.1X access.

Associating the Domain with PPP and Web Authentication Method Lists

- Run the **authentication ppp** command to associate the domain with a PPP authentication method list.
- Run the **authentication Web** command to associate the domain with a Web authentication method list.
- This configuration is mandatory if you need to apply a specified PPP or Web authentication method list to the domain.
- If no method list is associated to the domain, the default global method list is applied.

Associating the Domain with a Network Accounting Method List

- Run the **accounting network** command to associate the domain with a network accounting method.
- This configuration is mandatory if you need to apply a specified network accounting method list to the domain.
- If a domain is not associated with a network accounting method list, by default, the global default method list is used for accounting.

Associating the Domain with a Network Authorization Method List

- Run the **authorization network** command to associate the domain with a network authorization method list.
- This configuration is mandatory if you need to apply a specified network authorization method list to the domain.
- If a domain is not associated with a network authorization method list, by default, the global default method list is used for authorization.

Configuring the Domain Status

- Optional.
- When a domain is in Block state, the users in the domain cannot log in.
- By default, after a domain is created, its state is Active, indicating that all the users in the domain are allowed to request network services.

Configuring Whether to Contain the Domain Name in Usernames

- Optional.
- By default, the usernames exchanged between the NAS and an authentication server carry domain information.

Configuring the Maximum Number of Domain Users

- Optional.
- By default, the maximum number of access users allowed in a domain is not limited.

Verification

Run the **show aaa domain** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the AAA services. None of the rest of AAA commands can be effective if AAA is not enabled.

Enabling the Domain-Based AAA Service

Command	**aaa domain enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the domain-based AAA service. If there are authenticated users, enabling or disabling this function may cause accounting failures. In this case, you can run either command to restore accounting: 1. Run the **clear dot1x user all** command to trigger a new authentication for 802.1X authentication users automatically. 2. Run the **clear web-auth user all** command to log off Web authentication users. The users need to initiate authentication requests manually.

Creating a Domain and Entering Domain Configuration Mode

Command	**aaa domain** { **default** | *domain-name* }
Parameter Description	**default**: Uses this parameter to configure the default domain. *domain-name*: Indicates the name of the domain to be created.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a domain to provide the domain-based AAA service. The **default** parameter specifies the default domain. If a username does not carry domain information, the NAS uses the method list associated with the default domain to provide the AAA service to the user. The *domain-name* parameter specifies the name of the domain to be created. If the domain name carried by a username matches the configured domain name, the NAS uses the method list associated with this domain to provide the AAA service to the user. The system supports a maximum of 32 domains.

Associating the Domain with an 802.1X Authentication Method List

Command	**authentication dot1x** { **default** | *list-name* }

Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with an 802.1X authentication method list.

Associating the Domain with a Web Authentication Method List

Command	**authentication web-auth** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a Web authentication method list.

Associating the Domain with a Network Accounting Method List

Command	**accounting network** { **default |** *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a network accounting method list.

Associating the Domain with a Network Authorization Method List

Command	**authorization network** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	

Configuring the Domain Status

Command	**state** { **block** | **active** }
Parameter Description	**block**: Indicates that the configured domain is invalid. **active**: Indicates that the configured domain is valid.
Command Mode	Domain configuration mode
Usage Guide	Use this command to make the configured domain valid or invalid.

Configuring Whether to Contain the Domain Name in Usernames

Command	**username-format** { **without-domain** | **with-domain** }
Parameter Description	**without-domain**: Indicates to remove domain information from usernames. **with-domain**: Indicates to keep domain information in usernames.

Command Mode	Domain configuration mode
Usage Guide	Use this command in domain configuration mode to determine whether to include domain information in usernames when the NAS interacts with authentication servers in a specified domain.

Configuring the Maximum Number of Domain Users

Command	**access-limit** *num*
Parameter Description	*num*: Indicates the maximum number of access users allowed in a domain. This limit is applicable only to 802.1X STAs.
Command Mode	Domain configuration mode
Usage Guide	Use this command to limit the number of access users in a domain.

Configuration Example

Configuring the Domain-Based AAA Services

Configure authentication and accounting through a RADIUS server to 802.1X users (username: *user*@domain.com) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain information, and the number of access users is not limited.

Scenario Figure 1-13	
Configuration Steps	The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance. Step 1: Enable AAA. Step 2: Define an AAA method list. Step 3: Enable the domain-based AAA service. Step 4: Create a domain. Step 5: Associate the domain with the AAA method list. Step 6: Configure the domain attribute.
NAS	Hostname#configure terminal Hostname(config)#aaa new-model Hostname(config)#radius-server host 10.1.1.1 Hostname(config)#radius-server key test Hostname(config)#aaa authentication dot1x default group radius Hostname(config)#aaa accounting network list3 start-stop group radius Hostname(config)# aaa domain enable

	Hostname(config)# aaa domain domain.com Hostname(config-aaa-domain)# authentication dot1x default Hostname(config-aaa-domain)# accounting network list3 Hostname(config-aaa-domain)# username-format without-domain
Verification	Run the **show run** and **show aaa domain** commands on the NAS to display the configuration.
NAS	Hostname#show aaa domain domain.com ==========Domain domain.com========== State: Active Username format: With-domain Access limit: No limit 802.1X Access statistic: 0 Selected method list: authentication dot1x default accounting network list3
	Hostname#show run Building configuration... Current configuration : 1449 bytes version RGOS 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67) co-operate enable ! aaa new-model aaa domain enable ! aaa domain domain.com authentication dot1x default accounting network list3 ! aaa accounting network list3 start-stop group radius aaa authentication dot1x default group radius !

	nfpp ! no service password-encryption ! radius-server host 10.1.1.1 radius-server key test ! line con 0 line vty 0 4 ! end

Common Errors

N/A

1.4.6 Configuring a Policy for Accounting-Start Failures

Configuration Effect

- Configure a policy for accounting-start failures.

Notes

Configure a policy for accounting-start failures as required.

Configuration Steps

↘ Configuring a Policy for Accounting-Start Failures

- Optional
- By default, no policy is configured for accounting-start failures.

Verification

Run the **show run** to verify the configuration.

Related Commands

↘ Configuring a Policy for Accounting-Start Failures

Command	**aaa accounting start-fail** { **online** | **offline** }
Parameter Description	**online**: Allows the users that encounter accounting-start failures to be online. **offline**: Logs off the users that encounter accounting-start failures.
Command Mode	Global configuration mode

Usage Guide	Use this command to configure a policy for accounting-start failures.

Configuration Example

The following example involves configuration about only the policy for accounting-start failures.

Configure a policy for accounting-start failures.

Scenario Figure 1-14	
Configuration Steps	Configure a policy for accounting-start failures.
NAS	Hostname#configure terminal Hostname(config)#aaa accounting start-fail offline
Verification	Run the **show run** command on the NAS to display the configuration.
NAS	Hostname#sh run | inc aaa aaa accounting start-fail offline

Common Errors

N/A

1.4.7 Configuring Heartbeat Packet Detection

Configuration Effect

- Enable heartbeat packet detection. After this function is enabled, AAA processes and AAA databases can detect whether the peer end is available through heartbeat packets.

Notes

Heartbeat packet detection is supported only by some front-end AAA modules currently, including RADIUS and DOT1X modules.

Configuration Steps

Configuring Heartbeat Packet Detection

- Optional
- By default, heartbeat packet detection is enabled by default.

Verification

Run the **show run** command to verify the configuration.

Related Commands

Configuring Heartbeat Packet Detection

Command	[**no**] **aaa heartbeat enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable heartbeat packet detection.

Configuration Example

The following example involves configuration about only heartbeat packet detection.

Configuring Heartbeat Packet Detection

Scenario **Figure 1-15**	
Configuration Steps	Disable heartbeat packet detection.
NAS	Hostname#configure terminal Hostname(config)#no aaa heartbeat enable
Verification	Run the **show run** command on the NAS to display the configuration.
NAS	Hostname#sh run | inc heart no aaa heartbeat enable

Common Errors

N/A

1.4.8 Configuring AAA Logging

Configuration Effect

- Disable AAA logging or configure an AAA logging rate limit.

Notes

N/A

Configuration Steps

Configuring AAA Logging

- Optional
- By default, AAA logging is enabled.

Configure an AAA Logging Rate Limit

- Optional
- By default, five logs are printed per second.

Verification

Run the **show run** command to verify the configuration.

Related Commands

Configuring AAA Logging

Command	[**no**] **aaa log enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If numerous users get online, the incurred AAA logging may cause continuous screen refreshing or device performance decrease. You can configure this command to disable AAA logging.

Configuring an AAA Logging Rate Limit

Command	**aaa log rate-limit** *num*
Parameter Description	*num*: Configures a logging rate limit.
Command Mode	Global configuration mode
Usage Guide	If numerous users get online, the incurred AAA logging may cause continuous screen refreshing or device performance decrease. You can configure this command to configure a logging rate limit.

Configuration Example

The following example involves only configuration about AAA logging.

Configure AAA logging.

Scenario **Figure 1-16**	

Configuration Steps	Configure the device to print 10 logs per second.
NAS	Hostname# configure terminal Hostname(config)# aaa log enable Hostname(config)# aaa log rate-limit 10
Verification	Run the **show run** command on the NAS device to display the configuration
NAS	Hostname# show run | inc aaa log aaa log enable aaa log rate-limit 10

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the locked users.	**clear aaa local user lockout** {**all** | **user-name** *username* }

Displaying

Description	Command
Displays the accounting update information.	**show aaa accounting update**
Displays the current domain configuration.	**show aaa domain**
Displays the current lockout configuration.	**show aaa lockout**
Displays the AAA server groups.	**show aaa group**
Displays the AAA method lists.	**show aaa method-list**
Displays the AAA users.	**show aaa user**

1 Configuring RADIUS

1.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system.

RADIUS works with the Authentication, Authorization, and Accounting (AAA) to conduct identity authentication on users who attempt to access a network and prevent unauthorized access. In system implementation, a RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the central RADIUS server, where all user identity authentication information and network service information are stored. In addition to the authentication service, the RADIUS server provides authorization and accounting services for access users.

RADIUS is often applied in network environments that have high security requirements and allow the access of remote users. RADIUS is a completely open protocol and the RADIUS server is installed on many operating systems as a component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server currently.

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service is defined in the IETF RFC3576. This protocol defines a user offline management method. Devices communicate with the RADIUS server through the Disconnect-Messages (DMs) to bring authenticated users offline. This protocol implements compatibility between devices of different vendors and the RADIUS server in terms of user offline processing.

In the DM mechanism, the RADIUS server actively initiates a user offline request to a device, the device locates a user according to the user session information, user name, and other information carried in the request and brings the user offline. Then, the device returns a response packet that carries the processing result to the RADIUS server, thereby implementing user offline management of the RADIUS server.

Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 Applications

Application	Description
Providing Authentication, Authorization, and Accounting Services for Access Users	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.

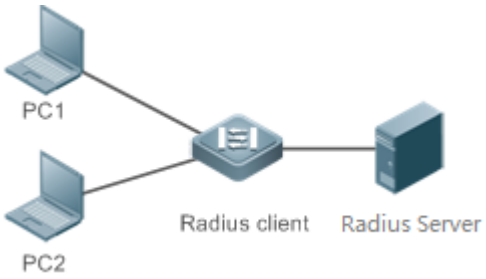
Application	Description
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

1.2.1 Providing Authentication, Authorization, and Accounting Services for Access Users

Scenario

RADIUS is typically applied in the authentication, authorization, and accounting of access users. A network device serves as a RADIUS client and transmits user information to a RADIUS server. After completing processing, the RADIUS server returns the authentication acceptance/authentication rejection/accounting response information to the RADIUS client. The RADIUS client performs processing on the access user according to the response from the RADIUS server.

Figure 1-1 Typical RADIUS Networking Topology



Remarks	PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, and initiate authentication and accounting requests. The RADIUS client is usually an access switch. The RADIUS server can be a component built in the Windows 2000/2003, Server (IAS), or UNIX operating system or dedicated server software provided by vendors.

Deployment

- Configure access device information on the RADIUS server, including the IP address and shared key of the access devices.
- Configure the AAA method list on the RADIUS client.
- Configure the RADIUS server information on the RADIUS client, including the IP address and shared key.
- Enable access control on the access port of the RADIUS client.
- Configure the network so that the RADIUS client communicates with the RADIUS server successfully.

1.2.2 Forcing Users to Go Offline

Scenario

The RADIUS server forces authenticated online users to go offline for the sake of management.

See Figure 1-1 for the networking topology.

Deployment

- Add the following deployment on the basis of 1.2.1 "Deployment".
- Enable the RADIUS dynamic authorization extension function on the RADIUS client.

1.3 Features

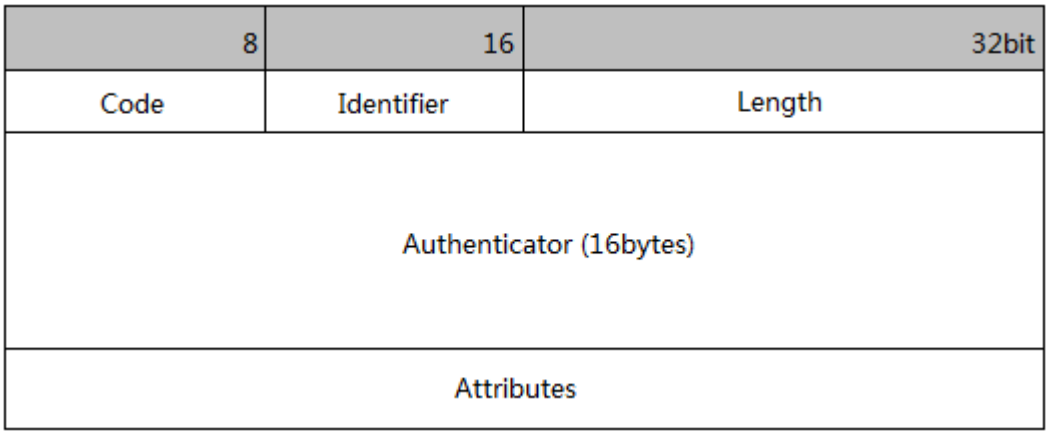
Basic Concepts

Client/Server Mode

- Client: A RADIUS client initiates RADIUS requests and usually runs on a device or NAS. It transmits user information to the RADIUS server, receives responses from the RADIUS server, and performs processing accordingly. The processing includes accepting user access, rejecting user access, or collecting more user information for the RADIUS server.
- Server: Multiple RADIUS clients map to one RADIUS server. The RADIUS server maintains the IP addresses and shared keys of all RADIUS clients as well as information on all authenticated users. It receives requests from a RADIUS client, conducts authentication, authorization, and accounting, and returns processing information to the RADIUS client.

Structure of RADIUS Packets

The following figure shows the structure of RADIUS packets.



- Code: Identifies the type of RADIUS packets, which occupies one byte. The following table lists the values and meanings.

Code	Packet Type	Code	Packet Type
1	Access-Request	4	Accounting-Request
2	Access-Accept	5	Accounting-Response
3	Access-Reject	11	Access-Challenge

- Identifier: Indicates the identifier for matching request packets and response packets, which occupies one byte. The identifier values of request packets and response packets of the same type are the same.

- Length: Identifies the length of a whole RADIUS packet, which includes **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes**. It occupies two bytes. Bytes that are beyond the **Length** field will be truncated. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.
- Authenticator: Verifies response packets of the RADIUS server by a RADIUS client, which occupies 16 bytes. This field is also used for encryption/decryption of user passwords.
- Attributes: Carries authentication, authorization, and accounting information, with the length unfixed. The **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type, Length, Value (TLV) format. Type occupies one byte and indicates the attribute type. The following table lists common attributes of RADIUS authentication, authorization, and accounting. Length occupies one byte and indicates the attribute length, with the unit of bytes. Value indicates the attribute information.

Attribute No.	Attribute Name	Attribute No.	Attribute Name
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token

Attribute No.	Attribute Name	Attribute No.	Attribute Name
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

Shared Key

A RADIUS client and a RADIUS server mutually confirm their identities by using a shared key during communication. The shared key cannot be transmitted over a network. In addition, user passwords are encrypted for transmission for the sake of security.

RADIUS Server Group

The RADIUS security protocol, also called RADIUS method, is configured in the form of a RADIUS server group. Each RADIUS method corresponds to one RADIUS server group and one or more RADIUS severs can be added to one RADIUS server group. For details about the RADIUS method, see the *Configuring AAA*. If you add multiple RADIUS servers to one RADIUS server group, when the communication between a device and the first RADIUS server in this group fails or the first RADIUS server becomes unreachable, the device automatically attempts to communicate with the next RADIUS server till the communication is successful or the communication with all the RADIUS servers fails.

RADIUS Attribute Type

- Standard attributes
- The RFC standards specify the RADIUS attribute numbers and attribute content but do not specify the format of some attribute types. Therefore, the format of attribute contents needs to be configured to adapt to different RADIUS server requirements. Currently, the format of the RADIUS Calling-Station-ID attribute (attribute No.: 31) can be configured.

The RADIUS Calling-Station-ID attribute is used to identify user identities when a network device transmits request packets to the RADIUS server. The RADIUS Calling-Station-ID attribute is a string, which can adopt multiple formats. It needs to uniquely identify a user. Therefore, it is often set to the MAC address of a user. For example, when IEEE 802.1X authentication is used, the Calling-Station-ID attribute is set to the MAC address of the device where the IEEE 802.1X client is installed. The following table describes the format of MAC addresses.

Format	Description
Ietf	Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC

Normal	Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac
Unformatted	Indicates the format without separators. This format is used by default. Example: 00d0f83322ac

- Private attributes

RADIUS is an extensible protocol. According to RFC2865, the Vendor-Specific attribute (attribute No.: 26) is used by device vendors to extend the RADIUS protocol to implement private functions or functions that are not defined in the standard RADIUS protocol. Table 1-3 lists private attributes supported by Ruijie products. The **TYPE** column indicates the default configuration of private attributes of Ruijie products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-Ruijie products.

ID	Function	TYPE	Extended TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	vlan-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	ipv6-multicast-address	79	79
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

Overview

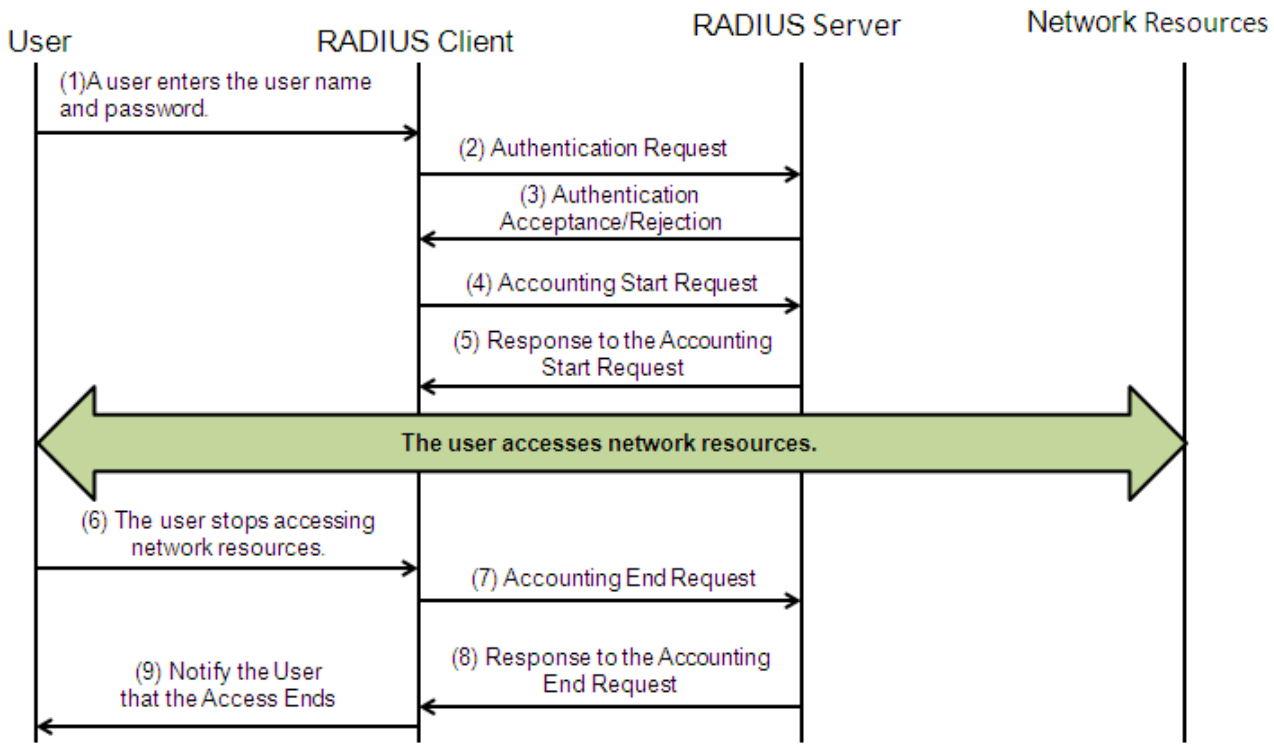
Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.
RADIUS Timeout Retransmission	Specifies the packet retransmission parameter for a RADIUS client when a RADIUS server does not respond to packets transmitted from the RADIUS client within a period of time.
RADIUS Server Accessibility Detection	Enables a RADIUS client to actively detect whether a RADIUS server is reachable and maintain the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.
RADIUS Forced Offline	Enables a RADIUS server to actively force authenticated users to go offline.
Configuring the DiffServ Code Point (DSCP) Value of RADIUS Packets	The DSCP field is contained in the Type of Service (ToS) field of IP packets. The DSCP value marks packet priority level for transmission. The default DSCP value of RADIUS packets is 0. You can specify the DSCP value for RADIUS packets using commands. A larger DSCP value represents a higher priority of RADIUS packets.
Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server	By default, the unit of data flows sent to the RADIUS server is bytes, and the unit of data packets sent to the RADIUS server is packets. You can specify the unit of data flows and data packets sent to the RADIUS server using commands.
RadSec Service	RadSec combines Transport Layer Security (TLS) and Transmission Control Protocol (TCP), which is securer than User Datagram Protocol (UDP) used for RADIUS transmission.

1.3.1 RADIUS Authentication, Authorization, and Accounting

Conduct identity authentication and accounting on access users, safeguard network security, and facilitate management for network administrators.

Working Principle

Figure 1-2



The RADIUS authentication and authorization process is described as follows:

1. A user enters the user name and password and transmits them to the RADIUS client.
2. After receiving the user name and password, the RADIUS client transmits an authentication request packet to the RADIUS server. The password is encrypted for transmission. For the encryption method, see RFC2865.
3. The RADIUS server accepts or rejects the authentication request according to the user name and password. When accepting the authentication request, the RADIUS server also issues authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.
4. The RADIUS accounting process is described as follows:
5. If the RADIUS server returns authentication acceptance information in Step (3), the RADIUS client sends an accounting start request packet to the RADIUS server immediately.
6. The RADIUS server returns the accounting start response packet, indicating accounting start.
7. The user stops accessing network resources and requests the RADIUS client to disconnect the network connection.
8. The RADIUS client transmits the accounting end request packet to the RADIUS server.
9. The RADIUS server returns the accounting end response packet, indicating accounting end.
10. The user is disconnected and cannot access network resources.

Related Configuration

Configuring RADIUS Server Parameters

No RADIUS server is configured by default.

You can run the **radius-server host** command to configure a RADIUS server.

At least one RADIUS server must be configured so that RADIUS services run normally.

Configuring the AAA Authentication Method List

No AAA authentication method list is configured by default.

You can run the **aaa authentication** command to configure a method list for different user types and select **group radius** when setting the authentication method.

The RADIUS authentication can be conducted only after the AAA authentication method list of relevant user types is configured.

Configuring the AAA Authorization Method List

No AAA authorization method list is configured by default.

You can run the **aaa authorization** command to configure an authorization method list for different user types and select **group radius** when setting the authorization method.

The RADIUS authorization can be conducted only after the AAA authorization method list of relevant user types is configured.

Configuring the AAA Accounting Method List

No AAA accounting method list is configured by default.

You can run the **aaa accounting** command to configure an accounting method list for different user types and select **group radius** when setting the accounting method.

The RADIUS accounting can be conducted only after the AAA accounting method list of relevant user types is configured.

1.3.2 Source Address of RADIUS Packets

Specify the source IP address used by a RADIUS client to transmit packets to a RADIUS server.

Working Principle

When configuring RADIUS, specify the source IP address to be used by a RADIUS client to transmit RADIUS packets to a RADIUS server, in an effort to reduce the workload of maintaining a large amount of NAS information on the RADIUS server.

Related Configuration

The global routing is used to determine the source address for transmitting RADIUS packets by default.

Run the **ip radius source-interface** command to specify the source interface for transmitting RADIUS packets. The device uses the first IP address of the specified interface as the source address of RADIUS packets.

1.3.3 RADIUS Timeout Retransmission

Working Principle

After a RADIUS client transmits a packet to a RADIUS server, a timer is started to detect the response of the RADIUS server. If the RADIUS server does not respond within a certain period of time, the RADIUS client retransmits the packet.

Related Configuration

↘ Configuring the RADIUS Server Timeout Time

The default timeout time is 5 seconds.

You can run the **radius-server timeout** command to configure the timeout time. The value ranges from 1 second to 1,000 seconds.

The response time of a RADIUS server is relevant to its performance and the network environment. Set an appropriate timeout time according to actual conditions.

↘ Configuring the Retransmission Count

The default retransmission count is 3.

You can run the **radius-server retransmit** command to configure the retransmission count. The value ranges from 1 to 100.

↘ Configuring Whether to Retransmit Accounting Update Packets

Accounting update packets are not retransmitted by default.

You can run the **radius-server account update retransmit** command to configure retransmission of accounting update packets for authenticated users.

1.3.4 RADIUS Server Accessibility Detection

Working Principle

A RADIUS client actively detects whether a RADIUS server is reachable and maintains the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.

Related Configuration

↘ Configuring the Criteria for the Device to Judge That a RADIUS Server Is Unreachable

The default criteria configured for judging that a RADIUS server is unreachable meet the two conditions simultaneously: 1. The device does not receive a correct response packet from the RADIUS security server within 60 seconds. 2. The device transmits the request packet to the same RADIUS security server for consecutive 10 times.

You can run the **radius-server dead-criteria** command to configure the criteria for the device to judge that the RADIUS security server is unreachable.

↘ Configuring the Test User Name for Actively Detecting the RADIUS Security Server

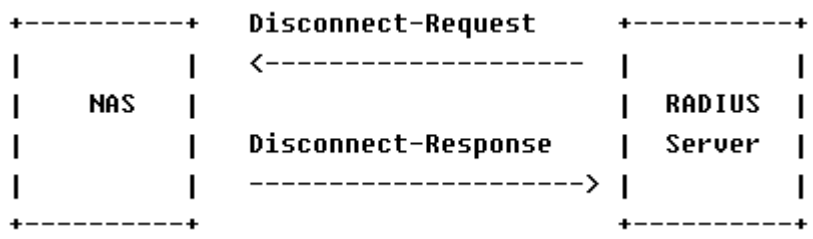
No test user name is specified for actively detecting the RADIUS security server by default.

You can run the **radius-server host x.x.x.xtestusername xxx** command to configure the test user name.

1.3.5 RADIUS Forced Offline

Working Principle

Figure 1-3 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol



The preceding figure shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request message to UDP Port 3799 of the device. After processing, the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

Related Configuration

N/A

1.3.6 Configuring the DiffServ Code Point (DSCP) Value of RADIUS Packets

Working Principle

The DSCP field is contained in the Type of Service (ToS) field of IP packets. The DSCP value marks packet priority level for transmission. The default DSCP value of RADIUS packets is 0. You can specify the DSCP value for RADIUS packets using commands. A larger DSCP value represents a higher priority of RADIUS packets.

Related Configuration

↘ Configuring the DSCP Value of RADIUS Packets

Run the **radius dscp** command to specify the DSCP value of RADIUS packets. The value ranges from 0 to 63.

1.3.7 Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server

Working Principle

By default, the unit of data flows sent to the RADIUS server is bytes, and the unit of data packets sent to the RADIUS server is packets. You can specify the unit of data flows and data packets sent to the RADIUS server using commands.

Related Configuration

↘ Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server

Run the **radius data-flow-format data** { **byte** | **kilo-byte** | **mega-byte** | **giga-byte** } **packet** { **one-packet** | **kilo-packet** | **mega-packet** | **giga-packet** } command to configure the unit of data flows and data packets sent to the RADIUS server.

1.3.8 RadSec Service

Working Principle

TLS RADIUS provides secure communication for RADIUS requests by using the TLS protocol. RADIUS on TLS (also called RadSec) redirects common RADIUS traffic to a remote RADIUS server through a TLS connection. RadSec allows RADIUS authentication, authorization, and accounting data to be securely transmitted over untrusted networks.

RadSec combines TLS and TCP, which is securer than UDP used for RADIUS transmission. UDP-based RADIUS encrypts shared keys by using the MD5 algorithm that is prone to attacks. RadSec uses an encrypted TLS tunnel to exchange valid load of RADIUS data packets, reducing the risk of attacks on the MD5 algorithm.

Related Configuration

↘ Configuration

A RadSec server is represented by a RadSec target. To configure RadSec, you must define a RadSec server as a target and redirect RADIUS traffic to the target. A RadSec target is identified by a unique ID. Multiple RadSec targets can be configured. Different parameters indicate the same RadSec server.

To redirect traffic from a standard RADIUS server to a RadSec server, associate the RADIUS server with the RadSec target. For example, to associate RADIUS server 10.1.1.1 with RadSec target 10, run the **radius-server host 10.1.1.1 radsec-destination 10** command.

1.4 Configuration

Configuration	Description and Command	
RADIUS Basic Configuration	⚠ (Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.	
	radius-server host	Configures the IP address of the remote RADIUS security server.
	radius-server key	Configures the shared key for communication between the device and the RADIUS server.
	radius-server retransmit	Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-server timeout	Configures the waiting time, after which the device retransmits a request.
	radius-server account update retransmit	Configures retransmission of accounting update packets for authenticated users.
	ip radius source-interface	Configures the source address of RADIUS packets.
Configuring the RADIUS Attribute Type	⚠ (Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.	
	radius-server attribute31	Configures the MAC address format of RADIUS attribute No. 31 (Calling-Station-ID).
	radius-server attribute class	Configures the parsing mode of the RADIUS Class attribute.
	radius set qoscos	Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the *Configuring QoS*.
	radius support cui	Configures the device to support the CUI attribute.
	radius vendor-specific	Configures the mode of parsing private attributes by the device.
	radius-server authentication attribute	Configures RADIUS authentication request packets to contain a specified attribute.
	radius-server account attribute	Configures RADIUS accounting request packets to contain a specified attribute.
	radius-server authentication vendor	Configures RADIUS authentication request packets to contain a vendor-specific attribute (VSA).
	radius-server account vendor	Configures RADIUS accounting request packets to contain a VSA.
Configuring RADIUS Accessibility Detection	⚠ (Optional) It is used to detect whether a RADIUS server is reachable and maintain the accessibility of the RADIUS server.	

Configuration	Description and Command	
	radius-server dead-criteria	Configures the global criteria for judging that a RADIUS security server is unreachable.
	radius-server deadtime	Configures the duration for the device to stop transmitting request packets to an unreachable RADIUS server.
	radius-server host	Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.
Configuring the DSCP Value of RADIUS Packets	**radius dscp**	Configures the DSCP value of RADIUS packets.
Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server	**radius data-flow-format data {byte | kilo-byte | mega-byte | giga-byte} packet {one-packet | kilo-packet | mega-packet | giga-packet}**	Configures the unit of data flows and data packets sent to the RADIUS server.
Configuring Attributes of the RadSec Target Server	(Mandatory) It is used to configure RadSec authentication, authorization, and accounting.	
	radsec destination	Configures RadSec attributes.

1.4.1 RADIUS Basic Configuration

Configuration Effect

- RADIUS authentication, authorization, and accounting can be conducted after RADIUS basic configuration is complete.

Notes

- Before configuring RADIUS on the device, ensure that the network communication of the RADIUS server is in good condition.
- When running the **ip radius source-interface** command to configure the source address of RADIUS packets, ensure that the device of the source IP address communicates with the RADIUS server successfully.
- When conducting RADIUS IPv6 authentication, ensure that the RADIUS server supports RADIUS IPv6 authentication.

Configuration Steps

↘ Configuring the Remote RADIUS Security Server

- Mandatory.
- Configure the IP address, authentication port, accounting port, and shard key of the RADIUS security server.

↘ Configuring the Shared Key for Communication Between the Device and the RADIUS Server

- Optional.
- Configure a shared key in global configuration mode for servers without a shared key.

⚠ The shared key on the device must be consistent with that on the RADIUS server.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

- Optional.
- Configure the request transmission count, after which the device confirms that a RADIUS server is unreachable, according to the actual network environment.

Configuring the Waiting Time, After which the Device Retransmits a Request

- Optional.
- Configure the waiting time, after which the device retransmits a request, according to the actual network environment.

⚠ In an 802.1X authentication environment that uses the RADIUS security protocol, if a network device serves as the 802.1X authenticator and Ruijie SU is used as the 802.1X client software, it is recommended that **radius-server timeout** be set to 3 seconds (the default value is 5 seconds) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

- Optional.
- Determine whether to enable the function of retransmitting accounting update packets of authenticated users according to actual requirements.

Configuring the Source Address of RADIUS Packets

- Optional.
- Configure the source address of RADIUS packets according to the actual network environment.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to confirm that the device communicates with the RADIUS server over the RADIUS protocol.

Related Commands

Configuring the Remote RADIUS Security Server

Command	**radius-server host** { *ipv4-address* | *ipv6-address*} [**auth-port***port-number*] [**acct-port***port-number*][**test username***name* [**idle-time***time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*] [**radsec-destination** id-number]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the RADIUS security server. *ipv6-address*: Indicates the IPv6 address of the RADIUS security server. **auth-port***port-number*: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct identity authentication.

	acct-port *port-number*: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct accounting. **test username** *name*: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection. **idle-time***time*: Indicates the interval for the device to transmit test packets to a reachable RADIUS security server. The default value is 60 minutes. The value ranges from 1 minute to 1,440 minutes (24 hours). **ignore-auth-port**: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default. **ignore-acct-port**: Disables the function of detecting the accounting port of the RADIUS security server. It is enabled by default. **key**[**0** | **7**] *text-string*: Configures the shared key of the server. The global shared key is used if it is not configured. **radsec-destination** id-number: Indicates the ID of the RadSec target to which traffic from the RADIUS server is redirected.
Command Mode	Global configuration mode
Usage Guide	A RADIUS security server must be defined to implement the AAA security service by using RADIUS. You can run the **radius-server host** command to define one or more RADIUS security servers.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

Command	**radius-server key** [**0** | **7**]*text-string*
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7**indicates simple encryption. The default value is **0**.
Command Mode	Global configuration mode
Usage Guide	A shared key is the basis for correct communication between the device and the RADIUS security server. The same shared key must be configured on the device and RADIUS security server so that they can communicate with each other successfully.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

Command	**radius-server retransmit***retries*
Parameter Description	*retries*: Indicates the RADIUS retransmission count. The value ranges from 0 to 100.
Command Mode	Global configuration mode
Usage Guide	The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count. There is an interval between consecutive two retransmissions.

Configuring the Waiting Time, After which the Device Retransmits a Request

Command	**radius-server timeout***seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the packet retransmission timeout time.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

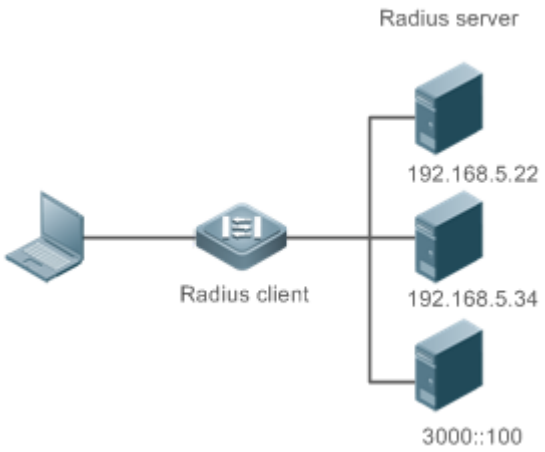
Command	**radius-server account update retransmit**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure retransmission of accounting update packets for authenticated users. Accounting update packets are not retransmitted by default. The configuration does not affect users of other types.

Configuring Sending of Accounting-on Packets upon NAS Restart

Command	**radius-server accounting-on enable**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Configure sending of accounting-on packets upon NAS restart. This function is enabled by default. Run the **no** form of this command to disable this function.

Configuration Example

Using RADIUS Authentication, Authorization, and Accounting for Login Users

Scenario **Figure 1-4**	
Configuration Steps	● Enable AAA. ● Configure the RADIUS server information.

	● Configure to use the RADIUS authentication, authorization, and accounting methods. ● Apply the configured authentication method on the interface.
RADIUS Client	Hostname#configure terminal Ruijie (config)#aaa new-model Ruijie (config)# radius-server host 192.168.5.22 Ruijie (config)#radius-server host 3000::100 Ruijie (config)# radius-server key aaa Ruijie (config)#aaa authentication login test group radius Ruijie (config)#aaa authorizationexectest group radius Ruijie (config)#aaa accountingexectest start-stop group radius Ruijie (config)# line vty 0 4 Ruijie (config-line)#login authentication test Ruijie (config-line)# authorization exec test Ruijie (config-line)# accounting exec test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. After obtaining a certain access level granted by the server, only run commands under this access level. Display the authentication log of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the accounting information on the user on the RADIUS server.
	Hostname#show running-config ! radius-server host 192.168.5.22 radius-server host 3000::100 radius-server key aaa aaa new-model aaa accounting exec test start-stop group radius aaa authorization exec test group radius aaa authentication login test group radius no service password-encryption iptcp not-send-rst ! vlan 1 ! line con 0

	line vty 0 4 accounting exec test authorization exec test login authentication test !

Common Errors

- The key configured on the device is inconsistent with that configured on the server.
- No method list is configured.

1.4.2 Configuring the RADIUS Attribute Type

Configuration Effect

- Define the attribute processing adopted when the device encapsulates and parses RADIUS packets.

Notes

- Private attributes involved in "Configuring the RADIUS Attribute Type" refer to Ruijie private attributes.

Configuration Steps

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

- Optional.
- Set the MAC address format of **Calling-Station-Id** to a type supported by the server.

Configuring the Parsing Mode of the RADIUS Class Attribute

- Optional.
- Configure the parsing mode of the Class attribute according to the server type.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

- Optional.
- Set the private attribute **port-priority** issued by the server to the COS value of an interface as required.

Configures the Device to Support the CUI Attribute

- Optional.
- Configure whether the device supports the RADIUS CUI attribute as required.

Configuring the Mode of Parsing Private Attributes by the Device

- Optional.
- Configure the index of a Ruijie private attribute parsed by the device as required.

Configuring RADIUS Authentication Request Packets to Contain a Specified Attribute

- Optional.
- Configure RADIUS authentication request packets to contain a specified attribute.

Configuring RADIUS Accounting Request Packets to Contain a Specified Attribute

- Optional.
- Configure RADIUS accounting request packets to contain a specified attribute.

Configuring RADIUS Authentication Request Packets to Contain a VSA

- Optional.
- Configure RADIUS authentication request packets to contain a VSA.

Configuring RADIUS Accounting Request Packets to Contain a VSA

- Optional.
- Configure RADIUS accounting request packets to contain a VSA.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

- Optional.
- Configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Configuring the NAS-Port-ID Encapsulation Format of RADIUS Packets

- Optional.
- Configure the NAS-Port-ID encapsulation format of RADIUS packets applicable to QinQ and non-QinQ scenarios. The default is the common encapsulation format.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to display the MAC address format of Calling-Station-Id.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that Ruijie private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that the CUI attribute is correctly parsed by the device.

Related Commands

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

Command	**radius-server attribute 31 mac format { ietf | normal | unformatted | dot-split | colon-split | hyphen-split }** [**mode1** | **mode2**] [**lowercase | uppercase**]
Parameter Description	**ietf**: Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC. **normal**: Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac.

	unformatted: Indicates the format without separators. This format is used by default. Example: 00d0f83322ac. **dot-split**: Indicates the format of MAC address. '.' is used as the separator. This parameter should be configured with **mode1** or **mode2**. **colon-split**: Indicates the format of MAC address. ':' is used as the separator. This parameter should be configured with **mode1** or **mode2**. **hyphen-split**: Indicates the format of MAC address. '-' is used as the separator. This parameter should be configured with **mode1** or **mode2**. **mode1**: Indicates the format of MAC address. Four characters make up one group. This parameter should be configured with **dot-split**, **colon-split**, or **hyphen-split**. For example: 00D0.F833.22AC, 00D0:F833:22AC, and 00D0-F833-22AC. **mode2**: Indicates the format of MAC address. Two characters make up one group. This parameter should be configured with **dot-split**, **colon-split**, or **hyphen-split**. For example: 00.D0.F8.33.22.AC, 00:D0:F8:33:22:AC, and 00-D0-F8-33-22-AC. **lowercase**: Indicates lowercase letters to be used in the MAC address. **uppercase**: Indicates uppercase letters to be used in the MAC address.
Command Mode	Global configuration mode
Usage Guide	Some RADIUS security servers (mainly used for 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the MAC address format of Calling-Station-ID to IETF.

Configuring the Parsing Mode of the RADIUS Class Attribute

Command	**radius-server attribute class user-flow-control** { **format-16bytes** | **format-32bytes** }
Parameter Description	**user-flow-control:** Parses the rate limit configuration from the class attribute. **format-16bytes:** Sets the format of the rate limit value to 16 bytes in the **class** attribute. **format-32bytes:** Sets the format of the rate limit value to 32 bytes in the **class** attribute.
Command Mode	Global configuration mode
Usage Guide	Configure this command if the server needs to issue the rate limit value by using the Class attribute.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

Command	**radius set qos cos**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to use the issued QoS value as the CoS value. The QoS value is used as the DSCP value by default.

Configures the Device to Support the CUI Attribute

Command	**radius support cui**
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	Configure this command to enable the RADIUS-compliant device to support the CUI attribute.

Configuring the Mode of Parsing Private Attributes by the Device

Command	**radius vendor-specific extend**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to identify attributes of all vendor IDs by type.

Configuring RADIUS Authentication Request Packets to Contain a Specified Attribute

Command	**radius-server authentication attribute** *type* **package** **radius-server authentication attribute** *type* **unpackage**
Parameter Description	*type*: Indicates the type of a RADIUS attribute. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure RADIUS authentication request packets to contain a specified attribute.

Configuring RADIUS Accounting Request Packets to Contain a Specified Attribute

Command	**radius-server account attribute** *type* **package** **radius-server account attribute** *type* **unpackage**
Parameter Description	*type*: Indicates the type of a RADIUS attribute. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure RADIUS accounting request packets to contain a specified attribute.

Configuring RADIUS Authentication Request Packets to Contain a VSA

Command	**radius-server authentication vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates a vendor name, including **cmcc**, **microsoft**, **cisco**, and **hw**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure RADIUS authentication request packets to contain a VSA.

Configuring RADIUS Accounting Request Packets to Contain a VSA

Command	**radius-server account vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates a vendor name, including **cmcc**, **microsoft**, **cisco**, and **hw**.
Command Mode	Global configuration mode

Usage Guide	Use this command to configure RADIUS accounting request packets to contain a VSA.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

Command	**radius vendor-specific attribute support** *vendor_name*
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to **cisco**, **huawei** or **ms**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Configuring the NAS-Port-ID Encapsulation Format of RADIUS Packets

Command	**radius-server attribute nas-port-id format** { **qinq** | **normal** | **port-vid** | **mode1**}
Parameter Description	**qinq**: Indicates encapsulating the NAS-Port-ID attribute based on a predefined combination of the interface name, inner VLAN ID (VID) and outer VID. **port-vid**: Indicates encapsulating the NAS-Port-ID attribute based on a predefined combination of the interface name and VID. **normal**: Indicates encapsulating the NAS-Port-ID attribute based on the interface name. **mode1**: Indicates encapsulating the NAS-Port-ID attribute in the following format: slot=XX; subslot=XX; port=XXX; VLAN ID=XXXX. The slot value ranges from 0 to 15; the subslot value ranges from 0 to 15; the port value ranges from 0 to 255; the VLAN ID ranges from 1 to 4094. If the port value exceeds 255, this format is not available.
Command Mode	Global configuration mode
Usage Guide	Configure the NAS-Port-ID encapsulation format of RADIUS packets applicable to QinQ and non-QinQ scenarios.

Configuration Example

Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	● Configure the MAC address format of RADIUS Calling-Station-Id. ● Set the QoS value issued by the RADIUS server as the COS value of the interface. ● Configure the RADIUS function to support the CUI attribute. ● Configure the device to support private attributes of other vendors. ● Configure RADIUS authentication request packets to not encapsulate the NAS-Port-ID attribute. ● Configure RADIUS accounting request packets to contain CMCC VSA. ● Configure the RADISU server not to parse Cisco VSA. ● Configure the NAS-Port-ID encapsulation format of RADIUS packets in the QinQ scenario.

	Hostname(config)#radius-server attribute 31 mac format ietf Hostname(config)#radius set qos cos Hostname(config)#radius support cui Hostname(config)#radius vendor-specific extend Hostname(config)# radius-server authentication attribute 87 unpackage Hostname(config)# radius-server account vendor cmcc package Hostname(config)# no radius vendor-specific attribute support cisco Hostname(config)# radius-server attribute nas-port-id format qinq
Verification	Conduct packet capture or display debug information of the device to check whether the RADIUS standard attributes and private attributes are encapsulated/parsed correctly.

1.4.3 Configuring RADIUS Accessibility Detection

Configuration Effect

The device maintains the accessibility status of each configured RADIUS server: reachable or unreachable. The device will not transmit authentication, authorization, and accounting requests of access users to an unreachable RADIUS server unless all the other servers in the same RADIUS server group as the unreachable server are all unreachable.

The device actively detects a specified RADIUS server. The active detection function is disabled by default. If the active detection function is enabled for a specified RADIUS server, the device will, according to the configuration, periodically transmits detection requests (authentication requests or accounting requests) to the RADIUS server. The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the active detection interval of the reachable RADIUS server (the default value is 60 minutes).
- For an unreachable RADIUS server, the interval is always 1 minute.

Notes

All the following conditions need to be met before the active detection function is enabled for a specified RADIUS server:

- The test user name of the RADIUS server is configured on the device.
- At least one tested port (authentication port or accounting port) of the RADIUS server is configured on the device.

If the following two conditions are all met, it is deemed that a reachable RADIUS server becomes unreachable:

- After the previous correct response is received from the RADIUS server, the time set in **radius-server dead-criteria time** *seconds* has elapsed.

- After the previous correct response is received from the RADIUS server, the count that the device transmits requests to the RADIUS server but fails to receive correct responses (including retransmission) reaches the value set in **radius-server dead-criteria tries** *number*.

If any of the following conditions is met, it is deemed that an unreachable RADIUS server becomes reachable:

- The device receives correct responses from the RADIUS server.
- The duration that the RADIUS server is in the unreachable state exceeds the time set in **radius-server deadtime** and the active detection function is disabled for the RADIUS server.
- The authentication port or accounting port of the RADIUS server is updated on the device.

Configuration Steps

Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

- Mandatory.
- Configuring the global criteria for judging that a RADIUS security server is unreachable is a prerequisite for enabling the active detection function.

Configuring the IP Address of the Remote RADIUS Security Server, Authentication Port, Accounting Port, and Active Detection Parameters

- Mandatory.
- Configuring active detection parameters of the RADIUS server is a prerequisite for enabling the active detection function.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

- Optional.
- The configured duration for the device to stop transmitting request packets to an unreachable RADIUS server takes effect only when the active detection function is disabled for the RADIUS server.

Verification

- Run the **show radius server** command to display the accessibility information of each RADIUS server.

Related Commands

Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

Command	**radius-server dead-criteria** { **time***seconds* [**tries***number*] | **tries***number* }
Parameter Description	**time***seconds*: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds. **tries***number*: Indicates the consecutive request timeout count. If the timeout count of request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.

Command Mode	Global configuration mode
Usage Guide	If a RADIUS security server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS security server is unreachable. Users can use this command to adjust parameter values in the duration condition and consecutive request timeout count condition.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

Command	**radius-server deadtime** *minutes*
Parameter Description	*minutes*: Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).
Command Mode	Global configuration mode
Usage Guide	If the active detection function is enabled for a RADIUS security server on the device, the time parameter in **radius-server deadtime** does not take effect on the RADIUS server. If the active detection function is disabled for a RADIUS security server, the device automatically restores the RADIUS security server to the reachable state when the duration that the RADIUS security server is in the unreachable state exceeds the time specified in **radius-server deadtime**.

Configuration Example

Configuring Accessibility Detection on the RADIUS Server

Scenario **Figure 1-5**	
Configuration Steps	● Configure the global criteria for judging that a RADIUS security server is unreachable. ● Configure the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.
RADIUS Client	Hostname(config)#radius-server dead-criteria time120 tries 5 Hostname(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
Verification	Disconnect the network communication between the device and the server with the IP address of 192.168.5.22.Conduct RADIUS authentication through the device. After 120 seconds, run the **show radius server** command to check that the server state is **dead**.
	Hostname#show running-config ... radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90 radius-server dead-criteria time 120 tries 5

	...

1.4.4 Configuring the DSCP Value of RADIUS Packets

Configuration Effect

- Configure the DSCP value of RADIUS packets.

Notes

- A larger DSCP value represents a higher priority of RADIUS packets.

Configuration Steps

↘ **Configuring the DSCP Value of RADIUS Packets**

- Optional.

Verification

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

Related Command

↘ **Configuring the DSCP Value of RADIUS Packets**

Command	**radius dscp** *dscp-value*
Parameter Description	*dscp-value*: Indicates the DSCP value.
Command Mode	Global configuration mode
Usage Guide	The value ranges from 0 to 63.

1.4.5 Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server

Configuration Effect

- Configure the unit of data flows and data packets sent to the RADIUS server.

Notes

- Specify the unit of data flows and data packets as required.

Configuration Steps

↘ **Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server**

- Optional.

Verification

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

Related Commands

Configuring the Unit of Data Flows and Data Packets Sent to the RADIUS Server

Command	**radius data-flow-format data {byte | kilo-byte | mega-byte | giga-byte} packet {one-packet | kilo-packet | mega-packet | giga-packet}**
Parameter Description	**byte**: Sets the unit of data flows to bytes. **kilo-byte**: Sets the unit of data flows to kilobytes. **mega-byt**: Sets the unit of data flows to megabytes. **giga-byte**: Sets the unit of data flows to gigabytes. **one-packet**: Sets the unit of data packets to packets. **kilo-packet**: Sets the unit of data packets to kilo-packets. **mega-packet**: Sets the unit of data packets to mega-packets. **giga-packet**: Sets the unit of data packets to giga-packets.
Command Mode	Global configuration mode
Usage Guide	Specify the unit of data flows and data packets as required.

1.4.6 Configuring Attributes of the RadSec Target Server

Configuration Effect

Use TLS to provide secure communication for RADIUS requests.

Notes

To configure RadSec, you must define a RadSec server as a target and redirect RADIUS traffic to the target.

Configuration Steps

Associating a RADIUS Server with a RadSec Target

- Mandatory.
- Configure a RadSec server as a target for traffic redirected from a standard RADIUS server.

Configuring RadSec Attributes

- Mandatory.
- Specifying RadSec server parameters is a prerequisite for enabling the RadSec function.

Verification

- Configure RADIUS traffic redirection and perform user authentication, authorization, and accounting.
- When the device exchanges data with a RadSec server, capture TLS packets.

- When the device exchanges data with a RADIUS server, view debugging information and check that exchange between the device and the RadSec server is normal.

Related Commands

Configuring RADIUS Attribute Types

Command	**radsec destination** *id-number* **host** *ipv4-address* [**port** *port-number*] **tls-certificate** *certificate-name* **tls-peer-name** *cert-server-name* [**tls-timeout** *seconds*]
Parameter Description	**Id-number:** Indicates a unique ID of a RadSec server. **ipv4-address**: Indicates the IP address of the RadSec target server. **port-number**: Indicates the port number of the RadSec server. **certificate-name**: Indicates the name of the local certificate used for TLS communication. **cert-server-name**: Indicates the name of the RadSec server for authentication. **seconds**: Configures the TLS connection timeout time, in seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure attributes of the RadSec target server as required.

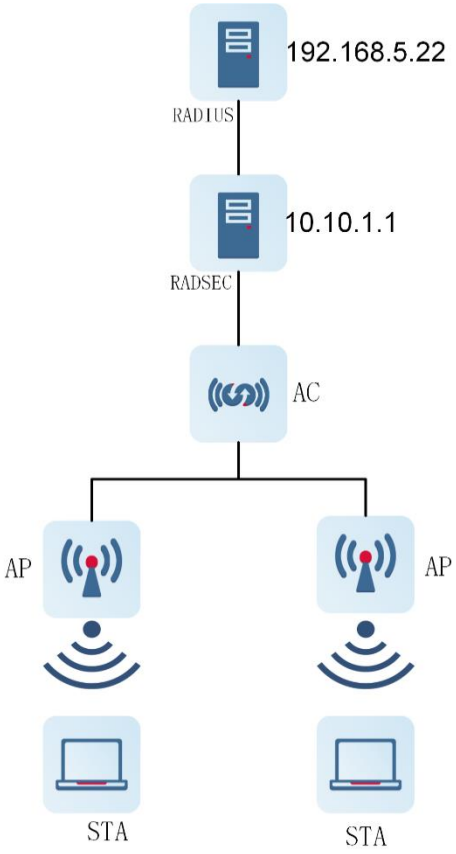
Configuration Example

The following configuration example describes RadSec-related configuration only.

Configuring RadSec Target Attributes

Scenario

Figure **1-6**



Prerequisites	1. Interfaces, IP addresses, and VLANs are configured in the network, the network is connected, and the route from the NAS device to the server is reachable. 2. PPSK authentication is enabled.
Configuration Steps	● Associate a RADIUS server with a RadSec target. ● Set the RadSec target unique ID to **10**, IP address to **10.10.1.1**, server port to **2022**, certificate name used for TLS communication to **my_cert**, server name for authentication to **x0.radsec.com**, and connection timeout time to 10s.

```
Hostname(config)# radius-server host 192.168.5.22 radsec-destination 10

Hostname(config)# radsec destination 10 host 10.10.1.1 port 2022 tls-certificate my_cert tls-peer-name x0.radsec.com tls-timeout 10
```

Verification

1. Capture packets or view debugging information to check whether TLS packet encapsulation or parsing is correct.
2. Run the **show radsec state** command to display the configuration.

```
Hostname# show radsec state

Radsec server ip        : 10.10.1.1

Radsec id number        : 10

Radsec server port      : 2022

Radsec server State : Active

tls-certificate         : my_cert

tls-peer-name           : x0.radsec.com

tls-timeout             : 10 Seconds
```

1.5 Monitoring

Clearing

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

Description	Command
Clears statistics of the RADIUS dynamic authorization extension function and restarts statistics.	**clear radius dynamic-authorization-extension statistics**

Displaying

Description	Command
Displays global parameters of the RADIUS server.	**show radius parameter**
Displays the configuration of the RADIUS server.	**show radius server**
Displays the configuration of the RADIUS private attribute type.	**show radius vendor-specific**
Displays statistics relevant to RADIUS authentication.	**show radius auth statistics**
Displays statistics relevant to RADIUS accounting.	**show radius acct statistics**
Displays configuration of RADIUS server groups.	**show radius group**
Displays RADIUS standard attributes.	**show radius attribute**
Displays statistics of a RadSec target.	**show radsec statistics**
Displays the RadSec connection status.	**show radsec state**

Debugging

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

Description	Command
Debugs the RADIUS event.	**debug radius event**
Debugs RADIUS packet printing.	**debug radius detail**
Debugs the RADIUS dynamic authorization extension function.	**debug radius extension event**
Debugs the RADIUS dynamic authorization extension packet printing.	**debug radius extension detail**

1 Configuring IEEE 802.1X

1.1 Overview

IEEE 802.1X is a standard for port-based network access control that provides secure access service for local area networks (LANs).

In IEEE 802-compliant LANs, users connecting to the network access devices (NASs) can access network resources without authentication and authorization, bringing security risks to the network. IEEE 802.1X was proposed to resolve security problems of such LANs.

802.1X supports three security applications: authentication, authorization, and accounting, which are called AAA.

- Authentication: Checks whether to allow user access and restricts unauthorized users.
- Authorization: Grants specified services to users and controls permissions of authorized users.
- Accounting: Records network resource status of users to provide statistics for charges.
- 802.1X can be deployed in a network to realize user authentication, authorization and other functions.

Protocols and Standards

- IEEE 802.1X: Port-Based Network Access Control

1.2 Applications

Application	Description
Wireless 802.1X Authentication	When an enterprise deploys a wireless LAN (WLAN), 802.1X authentication should be enabled on the Access Controller (AC).

1.2.1 Wireless 802.1X Authentication

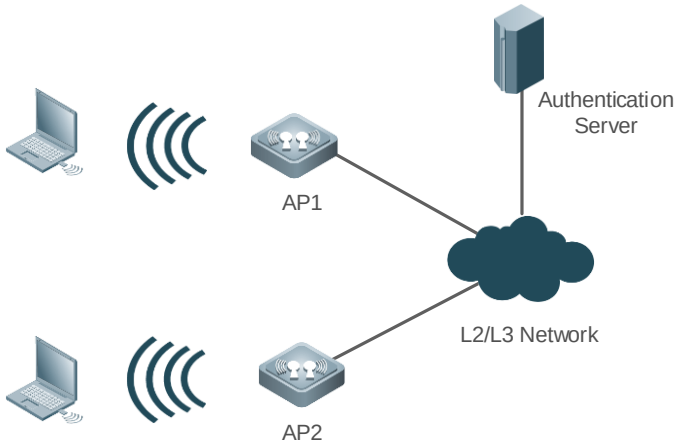
Scenario

An enterprise deploys wireless authentication - 802.1X on an AP for secure access control. Wireless stations (STAs) must pass 802.1X authentication to access the enterprise network.

As shown in the following figure:

- STAs are installed with 802.1X clients (which can come with the operating system, or others like Ruijie Supplicant).
- The AP supports 802.1X.
- One or multiple RADIUS servers perform authentication.

Figure 1-1



Remarks	Configure 802.1X authentication on the AP. STAs support 802.1X authentication. After connecting to APs, they will be authenticated through 802.1X. The RADIUS server runs the RADIUS server software to perform identity verification.

Deployment

- Enable 802.1X authentication on the AP based on the WLANs to make associated STAs controlled. Only authenticated STAs can access the network.
- Configure an AAA authentication method list so that 802.1X can adopt the appropriate method and authentication server.
- Configure RADIUS parameters to ensure proper communication between the AP and the RADIUS server. For details, see the *Configuring RDS*.
- If a Ruijie RADIUS server is used, configure SNMP parameters to allow the RADIUS server to manage devices, such as querying and setting.

1.3 Features

Basic Concepts

↘ User

802.1X is a LAN-based protocol. It identifies users based on physical information but not accounts. Except them, all other information such as the account ID and IP address can be changed. In WLANs, one MAC address represents an STA.

↘ RADIUS

RADIUS is a remote authentication protocol defined in RFC2865, which get wide practice. Using this protocol, the authentication server can remotely deploy and perform authentication. During 802.1X deployment, the authentication server is remotely deployed, and 802.1X authentication information between the NAS and the authentication server is transmitted through RADIUS.

↘ Timeout

During authentication, an NAS needs to communicate with the authentication client and server. If the authentication client or server times out, not responding within the time specified by 802.1X, authentication will fail. During deployment, ensure that the timeout specified by 802.1X is longer than that specified by RADIUS.

MAB

MAC address bypass (MAB) authentication means that the MAC address is used as the user name and password for authentication. Since Ruijie Supplicant cannot be installed on some dumb ends such as network printers, use MAB to perform security control.

EAP

802.1X uses Extensible Authentication Protocol (EAP) to carry authentication information. Defined in RFC3748, EAP provides a universal authentication framework, in which multiple authentication modes are embedded, including Message Digest Algorithm 5 (MD5), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Transport Layer Security (TLS). Ruijie 802.1X authentication supports various modes including MD5, CHAP, PAP, PEAP-MSCHAP, and TLS.

Authorization

- Authorization provides the following binding options for authentication users: IP address binding, VLAN binding, Access Control List (ACL) binding and Quality of Service (QoS) binding.

Accounting

Accounting performs network audit on network usage duration and traffic for users, which facilitates network operation, maintenance, and management.

Some RADIUS servers such as RG-SAM\RG-SMP servers need to check the online/offline status based on accounting packets. Therefore, accounting must be enabled on these RADIUS servers.

Overview

Feature	Description
Authentication	Provides secure admission for users. Only authenticated users can access the network.
Authorization	Grants network access rights to authenticated users, such as IP address binding and ACL binding
Accounting	Provides online record audit, such as online duration and traffic.

1.3.1 Authentication

Authentication aims to check whether users are authorized and prevent unauthorized users from accessing the network. Users must pass authentication to obtain the network access permission. They can access the network only after the authentication server verifies the account. Before user authentication succeeds, only EAPOL packets (Extensible Authentication Protocol over LAN, 802.1X packets) can be transmitted over the network for authentication.

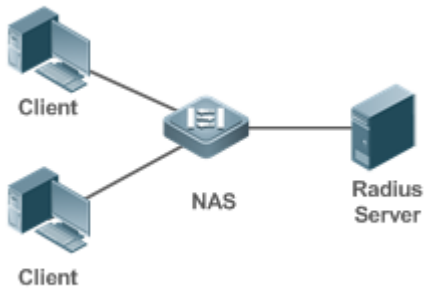
Working Principle

802.1X authentication is very simple. After a user submits its account information, the NAS sends the account information to the remote RADIUS server for identity authentication. If the authentication succeeds, the user can access the network.

Roles in Authentication

802.1X authentication involves three roles: supplicant, authenticator, and server. In real applications, their respective roles are client, network access server (NAS), and authentication server (mostly RADIUS server).

Figure 4-3



- Supplicant

The supplicant is the role of end users, usually a PC. It requests to access network services and replies to the request packets of the authenticator. The supplicant must run software compliant with the 802.1X standard. Except the typical 802.1X client support embedded in the operating system, Ruijie has launched a Ruijie Supplicant compliant with the 802.1X standard.

- Authenticator

The authenticator is usually an NAS such as a switch or wireless access hotspot. It controls the network connection of a client based on the client's authentication status. As a proxy between the client and the authentication server, the authenticator requests the user name from the client, verifies the authentication information from the authentication server, and forwards it to the client. Except as the 802.1X authenticator, the so-called NAS also acts as a RADIUS Client. It encapsulates the replies of the client into the RADIUS-format packets and forwards the packets to the RADIUS server. After receiving the information from the RADIUS server, it interprets the information and forwards it to the client.

The authenticator has two types of ports: controlled port and uncontrolled port. Users connected to controlled ports can access network resources only when authenticated. Users connected to uncontrolled ports can directly access network resources without authentication. We can connect users to controlled ports to control users. Uncontrolled ports are mainly used to connect the authentication server to ensure proper communication between the authentication server and the NAS.

- Authentication server

The authenticator server is usually an RADIUS server. It cooperates with the authenticator to provide authentication service for users. The authentication server saves the user names, passwords, and related authorization information. One server can provides authentication service for multiple authenticators to achieve centralized user management. The authentication server also manages accounting data received from

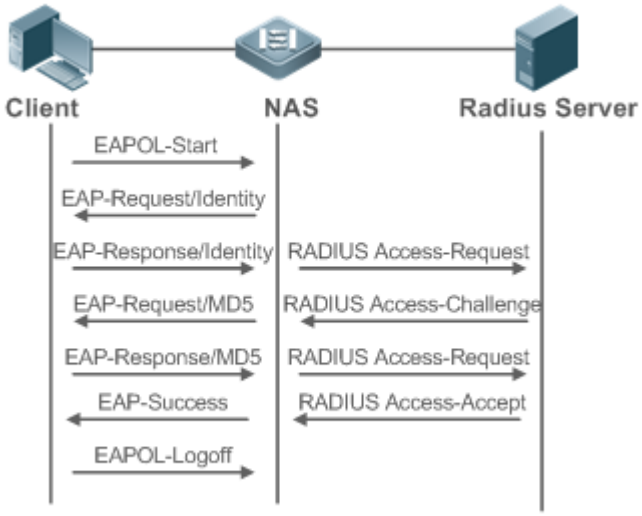
authenticators. Ruijie RADIUS servers compliant with 802.1X standard include Microsoft IAS/NPS, Free RADIUS Server, and Cisco ACS.

Authentication Process and Packet Exchange

The supplicant exchanges information with the authenticator through EAPOL while exchanges information with the authentication server through RADIUS. EAPOL is encapsulated on the MAC layer, with the type number of 0x888E. IEEE assigned a multicast MAC address 01-80-C2-00-00-03 for EAPOL to exchange packets during initial authentication. Ruijie Supplicant may also use 01-D0-F8-00-00-03 to for initial authentication packets.

Figure 4-4shows the typical authentication process of a wired user.

Figure 4-4



This is a typical authentication process initiated by a user. In special cases, the NAS, may take place of the user to initiate an authentication request.

Authenticating User Status

802.1X determines whether a user on a port can access the network based on the authentication status of the port. Ruijie products extend the 802.1X and realizes access control based on users (identify a wired user by the MAC address and VLAN ID while an STA by the MAC address) by default. Ruijie 802.1X can also be enabled in interface configuration mode. For details, see the chapter "Configuration."

All users on an uncontrolled port can access network resources, while users on a controlled port can access network resources only after authorized. When a user initiates authentication, its status remains Unauthorized and cannot access the network yet. After it passes authentication, its status changes to Authorized and can access network resources.

If the user connected to a controlled port does not support 802.1X, it will not respond to the NAS requesting the user name of the user. That means, the user remains Unauthorized and cannot access network resources.

In the case of 802.1X-enabled user and 802.1X-disabled NAS, if the user does not receive any responses after sending a specified number of EAPOL-Start packets, it regards the connected port uncontrolled and directly accesses network resources.

On 802.1X-enabled devices, all ports are uncontrolled by default. We can configure a port as controlled so that all users on this port have to be authorized.

If a user passes authentication (that is, the NAS receives a success packet from the RADIUS server), the user becomes Authorized and can freely access network resources. If the user fails in authentication, it remains Unauthorized and re-initiates authentication. If the communication between the NAS and the RADIUS server fails, the user remains Unauthorized and cannot access network resources.

When a user sends an EAPOL-LOGOFF packet, the user's status changes from Authorized to Unauthorized.

When a port becomes LINK-DOWN, all users connected to the port are unauthorized.

When the NAS restarts, all users on it become Unauthorized.

To enforce an STA to be exempted from authentication, you are advised to add a static MAC address or configure an IP-MAC binding.

↘ Deploying the Authentication Server

802.1X authentication uses the RADIUS server as the authentication server. Therefore, when 802.1X secure admission is deployed, the RADIUS server also needs to be deployed. Common RADIUS servers include Microsoft IAS/NPS, Cisco ACS, and RG-SAM/SMP. For details about the deployment procedure, see related software description.

↘ Configuring Authentication Parameters

To use 802.1X authentication, enable 802.1X authentication on the access port and configure AAA authentication method list and RADIUS server parameters. To ensure the accessibility between the NAS and RADIUS server, the 802.1X server timeout should be longer than the RADIUS server timeout.

↘ Supplicant

A user should start Ruijie Supplicant to enter the user name and initiate authentication. If the operating system brings an own authentication client and the network is available, a dialog box will be displayed, asking the user to enter the user name. Different clients may have different implementation processes and Graphical User Interfaces (GUIs). It is recommended to use Ruijie Supplicant as the authentication client. If other software is used, see related software description.

↘ Offline

If a user does not want to access the network, it can choose to go offline by multiple approaches, such as powering off the device, connecting the port to the network, and offline function provided by some supplicants.

↘ VLAN Hopping

After passing 802.1X authentication, a user is added to the VLAN assigned by the server. Then the user is allowed to communicate within that VLAN.

1.3.2 Authorization

After a user passes authentication, the NAS restricts the accessible network resources of the user in multiple approaches, such as accessible VLANs

Working Principle

Authorization means to bind the permissions with the users. A user is identified based on the MAC address and VLAN ID, as mentioned before. Besides MAC-VID binding, some other information such as the IP address and VLAN ID are bound with a user to implement authorization.

IP Authorization

The 802.1X authentication standard does not support IP identification. Ruijie 802.1X authentication extends 802.1X application and supports IP-MAC binding, which is called IP authorization. There are four IP authorization modes:

Supplicant authorization: An IP address is provided by the supplicant. This authorization mode is based on Ruijie supplicants.

RADIUS authorization: An IP address is delivered by a RADIUS server to the device after authentication succeeds.

Dynamic Host Configuration Protocol (DHCP) authorization: An authentication user initiates a DHCP Request message. After the user obtains an IP address, the device binds the IP address to the user's MAC address. DHCP authorization is applicable to a dynamic IP address scenario.

Mixed authorization: The device completes IP-MAC binding for an authentication user based on the sequence of supplicant authorization, RADIUS authorization, and DHCP authorization. If the supplicant provides an IP address, the IP address prevails. If not, the IP address provided by the RADIUS server is used. If the RADIUS server does not provide an IP address, the IP address provided by the DHCP server is used.

ACL Authorization

After user authentication is complete, the authentication server delivers the ACL or ACE to users. The ACL must be configured on the authentication server before delivery while no extra configuration is required for ACE delivery. ACL authorization delivers the ACL based on RADIUS attributes such as standard attributes, Ruijie-proprietary attributes, and Cisco-proprietary attributes. For details, see the software description related to the RADIUS server.

VLAN Authorization

Before a user passes authentication, the user belongs to the default VLAN of the VLAN group mapped to the access WLAN. The user is authenticated in the default VLAN. After the user passes authentication, the packets from the user are redirected to the VLAN delivered by the authentication server. If the authentication server does not deliver a VLAN, the packets from the user are transmitted in the default VLAN.

Logoff

The 802.1X authentication server can be used with Ruijie SAM or SMP to disconnect online users. The disconnected users are not allowed to access the network. This function can be used to control online duration and monitor accounting in real time.

1.3.3 Accounting

Accounting allows the network operators to audit the network access or fees of accessed users, including the online time and traffic.

Working Principle

Accounting is enabled on the NAS. The RADIUS server supports RFC2869-based accounting. When a user goes online, the NAS sends an accounting start packet to the RADIUS server which then starts accounting. When the user goes offline, the NAS sends an accounting end packet to the RADIUS server which then completes the accounting and generates a network fee accounting list. Different servers may perform accounting in different ways. Moreover, not all servers support accounting. Therefore, refer to the usage guide of the authentication server during actual deployment and accounting.

Accounting Start

After a user passes authentication, the accounting-enabled switch sends the RADIUS server an accounting start packet carrying user accounting attributes such as user name and accounting ID. After receiving the packet, the RADIUS server starts accounting.

Accounting Update

The NAS periodically sends Accounting Update packets to the RADIUS server, making the accounting more real-time. The accounting update interval can be provided by the RADIUS server or configured on the NAS.

Accounting End

After a user goes offline, the NAS sends the RADIUS server an accounting end packet carrying the online period and traffic of the user. The RADIUS server generates online records based on the information carried in this packet.

1.4 Configuration

Configuration	Description and Command	
Configuring 802.1X Basic Functions	⚠ (Mandatory) It is used to configure basic authentication and accounting.	
	aaa new-model	Enables AAA.
	aaa authentication dot1x	Configures an AAA authentication method list.
	aaa accounting networks	Configures an AAA accounting method list.
	radius-server host	Configures the RADIUS server parameters.
	radius-server key	Configures the pre-shared key for communication between the NAS and the RADIUS server.
Configuring VLAN	⚠ (Mandatory)	

Authorization	**vlan-group** *vlan-group-id*	Creates a VLAN group.
	vlan-list *vlan-list*	Configures VLAN members of a VLAN group.
	vlan-assign-mode	Configures a VLAN assignment mode for a VLAN group.
	default-vlan *vlan-id*	Configures a member VLAN of the VLAN group as the default VLAN delivered by the RADIUS server upon 802.1X authentication success.
Configuring 802.1X Parameters	⚠ (Optional) It is used to configure 802.1X parameters. ⚠ Ensure that the 802.1X server timeout is longer than the RADIUS server timeout. ⚠ Online Ruijie client detection applies only to Ruijie Supplicant.	
	dot1x re-authentication	Enables re-authentication.
	dot1x timeout re-authperiod	Configures the re-authentication interval.
	dot1x timeout tx-period	Configures the interval of EAP-Request/Identity packet retransmission.
	dot1x reauth-max	Configures the maximum times of EAP-Request/Identity packet retransmission.
	dot1x timeout supp-timeout	Configures the interval of EAP-Request/Challenge packet retransmission.
	dot1x max-req	Configures the maximum times of EAP-Request/Challenge packet retransmission.
	dot1x timeout server-timeout	Configures the authentication server timeout.
	dot1x timeout quiet-period	Configures the quiet period after authentication fails.
	dot1x auth-mode	Specifies the authentication mode (EAP/CHAP/PAP).
	dot1x client-probe enable	Configures connection status detection for Ruijie supplicants.
	dot1x probe-timer interval	Configures a detection interval for Ruijie supplicants.
	dot1x probe-timer alive	Configures a detection timer for Ruijie supplicants.
Configuring MAB	**dot1x-mab**	Enabling WLAN-based MAB
	dot1x mab-username upper	Enabling Uppercase Letters in MAB User Names

Configuring Extended Functions	(Optional) It is used to configure the trusted host list. (Optional) It is used to configure the device to send a forged MAC address. (Optional) It is used to configure multi-account authentication with one MAC address.	
	dot1x pseudo source	Configures the device to use the virtual MAC address as the source MAC address of the 802.1X packets from the device.
	dot1x multi-account enable	Enables multi-account authentication with one MAC address.
	dot1x valid-ip-acct enable	Enables IP-triggered accounting.
	dot1x valid-ip-acct timeout	Configures the timeout of obtaining IP addresses after users get authenticated. If timeout is reached, they will be kicked off.
	dot1x encryption only	Configures 802.1X authentication for encryption only when 802.1X and Web authentication are both enabled.
	dot1x logging rate-limit	Limits the rate of printing online and offline logs.
	dot1x offline-detect	Enables traffic detection on users in WLAN.
	dot1x user-trap enable	Enables SNMP trap during online and offline.
	dot1x domain-name	Configures a domain name for 802.1X authentication.

1.4.1 Configuring 802.1X Basic Functions

Configuration Effect

- Enable basic authentication and accounting services.
- On a wired network, run the **dot1x port-control auto** command in interface configuration mode to enable 802.1X authentication on a port.
- Run the **radius-server host** *ip-address* command to configure the IP address and port information of the RADIUS server and the **radius-server key** command to configure the RADIUS communication key between the NAS and the RADIUS server to ensure secure communication.
- Run the **aaa accounting update** command in global configuration mode to enable accounting update and the **aaa accounting update interval** command on the NAS to configure the accounting update interval. If the RADIUS server supports accounting update, you can also configure it on the RADIUS server. Prefer to use the parameters assigned by the authentication server than the parameters configured on the NAS.

Notes

- Configure accurate RADIUS parameters so that the basic RADIUS communication is proper.
- The 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, errors may occur during authentication and accounting.
- 802.1X uses the default method list by default. If the default method list is not configured for AAA, run the **dot1x authentication** and **dot1x accounting** commands to reconfigure it.
- When RG-SAM/SMP is used, accounting must be enabled. Otherwise, the RADIUS server will fail to detect users going offline, causing offline users remaining in the online user table.

Configuration Steps

↘ Enabling AAA

- (Mandatory) 802.1X authentication and accounting take effect only after AAA is enabled.
- Enable AAA on the NAS that needs to control user access by 802.1X.

Command	**aaa new-model**
Parameter Description	N/A
Defaults	AAA is disabled by default.
Command Mode	Global configuration mode
Usage Guide	AAA is disabled by default. This command is mandatory for the deployment of 802.1X authentication.

↘ Enabling an AAA Authentication Method List

- Mandatory.
- The AAA authentication method list must be consistent with the 802.1X authentication method list.
- Enable an AAA authentication method list after 802.1X authentication is enabled on the NAS.

Command	**aaa authentication dot1x** *list-name* **group radius**
Parameter Description	*list-name*: Indicates the 802.1X authentication method list of AAA.
Defaults	No AAA authentication method list is configured by default.
Command Mode	Global configuration mode
Usage Guide	AAA authentication modes are disabled by default. The AAA authentication mode must be consistent with the 802.1X authentication mode.

Command	**aaa accounting network** {**default**|*list-name*}**start-stop** *method1* [*method2*...]
Parameter Description	**default**: Indicates that the defined method list is the default method list for network accounting. *list-name:* Defines the name of a command accounting method list. It can be a string of any characters. **start-stop**: Sends accounting packets upon start and end of a user's access activity. The user is

	allowed to access the Internet whether accounting on the start of the access activity succeeds or not. *method*: Indicates keyword **none** or **group**. A method list contains up to four methods. **none**: Indicates that network accounting is not performed. **group**: Indicates that network accounting is performed through a server group. RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The device performs accounting of users' access activities by sending record attributes to the security server. Use keyword **start-stop** to specify accounting options.

Configuring the RADIUS Server Parameters

- (Mandatory) The RADIUS server parameters must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure RADIUS server parameters after 802.1X authentication is enabled on the NAS.

Command	**radius-server host** *ip-address* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server. *port1*: Indicates the authentication port. *port2*: Indicates the accounting port.
Defaults	No RADIUS server parameters are configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Pre-shared Key for Communication between the NAS and RADIUS Server

- (Mandatory) The pre-shared key for communication between the NAS and RADIUS server must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure the pre-shared key of the RADIUS server after 802.1X authentication is enabled on the NAS.

Command	**radius-server key** *string*
Parameter Description	*string*: Indicates the pre-shared key.
Defaults	No pre-shared key is configured for communication between the NAS and RADIUS server by default.
Command Mode	Global configuration mode
Usage Guide	The IP address of the NAS must be the same as that registered on the RADIUS server. The pre-shared key on the NAS must be the same as that on the RADIUS server. If the default RADIUS communication ports are changed on the RADIUS server, you need to change the communication ports on the NAS correspondingly.

Configuring Wireless 802.1X Authentication

- Mandatory.
- Configure this function on the AP.

- A WLAN enabled with 802.1X allows only 802.11 management frames and EAP packets to pass through. The other packets are discarded.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables the Robust Security Network (RSN) authentication mode. **disable**: Disables the RSN authentication mode.
Defaults	The RSN authentication mode is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	You can configure the encryption and authentication methods in RSN mode only after enabling the RSN authentication mode. Otherwise, the configuration does not take effect. The RSN authentication mode requires configuration of encryption and authentication methods. If you configure either encryption or authentication method (or neither), the wireless supplicant cannot access the WLAN.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Indicates the Advanced Encryption Standard (AES) encryption algorithm. **tcp**: Indicates the Temporal Key Integrity Protocol (TKIP) encryption algorithm. **enable**: Enables encryption for the RSN authentication mode. **disable**: Disables encryption for the RSN authentication mode.
Defaults	Encryption is not configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to configure encryption methods for the RSU authentication mode. Two encryption methods are available: AES and TKIP. In WLAN security configuration mode, both AES and TKIP encryption can be enabled.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable | disable** }
Parameter Description	**psk**: Indicates pre-shared key authentication. **802.1X**: Indicates 802.1X authentication. **enable**: Enables authentication for the RSN authentication mode. **disable**: Disables authentication for the RSN authentication mode.
Defaults	Authentication is not configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	You can configure the authentication method only after enabling the RSN authentication mode. In WLAN security configuration mode, only one authentication method can be enabled.

Verification

Start Ruijie Supplicant, enter the correct account information, and initiate authentication. Then check whether the 802.1X and RADIUS configurations are correct.

Checking for 802.1X Authentication Entries

Command	**show dot1x summary**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display entries of authenticated users to check the authentication status of users, for example, authenticating, authenticated, or quiet.
Command Display	Hostname#show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-state Port-Status User-Type Time --------- ---------- -------------- --------- ---- --------------- ------------- ----------- --------- ----------------- 16777302 ts-user b048.7a7f.f9f3 wlan 1 1 Authenticated Idle Authed static 0days 0h 0m12s

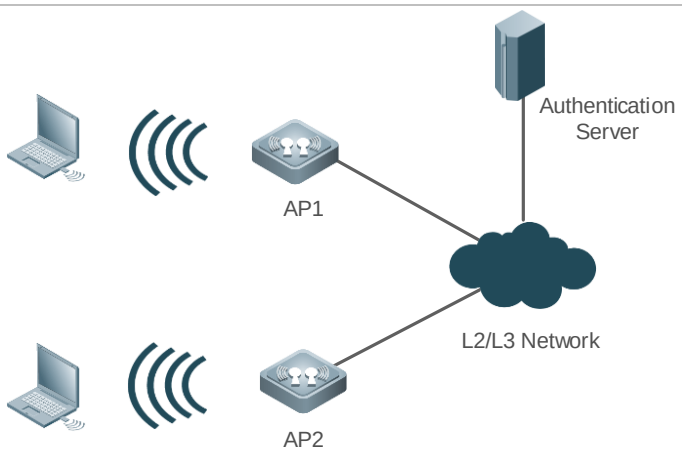
Checking for AAA User Entries

Command	**show aaa user all**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display information of AAA users.
Command Display	Hostname#show aaa user all ------------------------------ Id ----- Name 901 wwxy ------------------------------

- Check whether the RADIUS server responds to authentication based on the RADIUS packets between the NAS and the RADIUS server. If no, it means that the network is disconnected or parameter configurations are incorrect. If the RADIUS server directly returns a rejection reply, check the log file on the RADIUS server to identify the cause, e.g., of the authentication mode of the authentication server is incorrectly configured.

Configuration Example

Configuring 802.1X Authentication on a WLAN

Scenario **Figure 1-2**	
Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable 802.1X authentication on ports of the NAS. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	Hostname# configure terminal ruijie (config)# aaa new-model ruijie (config)# radius-server host 192.168.32.120 ruijie (config)# radius-server key ruijie ruijie (config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm 802.1x enable
Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username:tests-user,password:test**. ● The user fails to ping 192.168.32.120 before authentication. ● After the user enters account information and click **Authenticate** on Ruijie Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --------- ---------- -------------- --------- ---- --------------- ------------- ----------- --------- ------------------ 16778217 ts-user 0023.aeaa.4286 wlan 1 2 Authenticated Idle Authed static 0days 0h 0m 7s

Common Errors

- RADIUS parameters are incorrectly configured.
- The RADIUS server has a special access policy, for example, the RADIUS packets must carry certain attributes.
- The AAA authentication mode list is different from the 802.1X authentication mode list, causing authentication failure.

1.4.2 Configuring VLAN Authorization

Configuration Effect

- 802.1X authentication users transmit service data over the VLAN authorized by the server.

Configuration Steps

↘ Creating a VLAN Group

- Mandatory.
- Create a VLAN group to assign VLANs to STAs accessing a WLAN network.

Command	**vlan-group** *vlan-group-id*
Parameter Description	*vlan-group-id*: Indicates the VLAN group ID. The value ranges from 1 to 128.
Defaults	No VLAN group is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring VLAN Members of a VLAN Group

- Mandatory. Make sure that the VLAN has been created.
- If a WLAN is mapped to multiple VLANs, add these VLANs to a VLAN group.
- Configure this function on the AP.

Command	**vlan-list** *vlan-list*
Parameter Description	*vlan-list*: Indicates the VLAN member list. A list contains up to 128 members.
Defaults	A VLAN group contains no members by default.
Command Mode	VLAN group configuration mode
Usage Guide	N/A

↘ Configuring a VLAN Assignment Mode for a VLAN Group

- Mandatory.
- It is used to configure a VLAN assignment policy for a VLAN group.
- Configure this function on the AP.

Command	**vlan-assign-mode dot1x**
Parameter Description	**dot1x**: Indicates that the authentication server delivers the VLAN to users after 802.1X authentication succeeds.
Defaults	No VLAN assignment mode is configured for a VLAN group by default.
Command Mode	Global configuration mode or VLAN group configuration mode
Usage Guide	Global configuration applies to all VLAN groups. VLAN group configuration applies to only the current VLAN group. VLAN group configuration takes precedence over global configuration.

Configuring the Default VLAN for 802.1X Authentication Users Before Successful Authentication

- This command is mandatory if the VLAN assignment mode is 802.1X.
- If the VLAN assignment mode is 802.1X, the authentication server delivers the default VLAN to users upon authentication success.
- Configure this function on the AP.

Command	**default-vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates the default VLAN for 802.1X authentication users before they pass the authentication.
Defaults	No default VLAN is configured by default.
Command Mode	VLAN group configuration mode
Usage Guide	Before configuring the default VLAN, add this VLAN to the VLAN group.

Creating a WLAN Instance

- Mandatory.

Command	**dot11 wlan** *wlan-id*
Parameter Description	*wlan-id*: Indicates the WLAN instance ID. The value range is subject to the product.
Defaults	No WLAN instance is configured by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to create a WLAN instance and enter the WLAN instance configuration mode.

Creating a Wireless Sub-Interface

- Mandatory.

Command	**interface dot11radio** *interface-number* **.** *sub-interface-number*
Parameter	**dot11radio** *interface-number* **.** *Sub-interface-number*: Indicates a wireless sub-interface. The value

Description	range is subject to the product.
Defaults	No wireless sub-interface is configured by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to create a wireless sub-interface and enter the sub-interface configuration mode.

Configuring a Wireless Sub-Interface to Encapsulate the VLAN Group ID to Packets

- Mandatory.

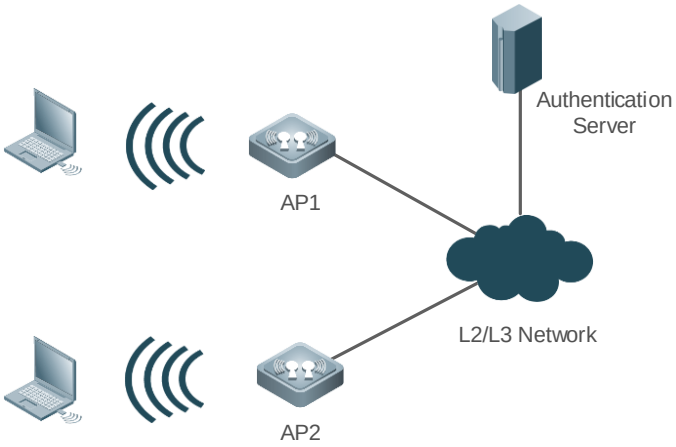
Command	**encapsulation dot1q** { *vlan-id* | **group** *vlan-group-id* }
Parameter Description	*vlan-id*: Indicates VLAN encapsulation on a sub-interface. The value ranges from 1 to 4094. For details, see *Configuring VLAN.* *vlan-group-id*: Indicates VLAN group ID encapsulated into packets on a sub-interface. The value ranges from 1 to 128.
Defaults	The interface or sub-interface does not encapsulate the VLAN ID or VLAN group ID to packets by default.
Command Mode	Sub-interface configuration mode
Usage Guide	N/A

Verification

- Run the **show vlan-group** to check the VLAN group configuration.

Configuration Example

Configuring VLAN Authorization

Scenario Figure 1-3	
Configuration Steps	● Create a VLAN group. 1. Configure 802.1X mode as the VLAN assignment mode for VLAN group 1 that contains VLANs 10 to 15. Specify VLAN 10 as the default VLAN.
	Hostname# configure terminal Hostname# configure terminal Hostname(config)# aaa new-model Hostname(config)# radius-server host 192.168.32.120 Hostname(config)# radius-server key key123

	Hostname(config)# aaa authentication dot1x default group radius Hostname(config)# aaa accounting network default start-stop group radius Hostname(config)# vlan-group 1 Hostname(config-vlan-group)# vlan-assign-mode dot1x Hostname(config-vlan-group)# vlan-list 10-15 Hostname(config-vlan-group)# default-vlan 10 Hostname(config-vlan-group)# exit ● Create a WLAN instance. Hostname(config)# dot11 wlan 1 Hostname(dot11-wlan-config)# ssid test Hostname(dot11-wlan-config)# exit ● Configure the mapping between the WLAN instance and the VLAN group. Hostname(config)# interface dot11radio 1/0 Hostname(config-if-Dot11radio 1/0)# encapsulation dot1Q group 1 Hostname(config-if-Dot11radio 1/0)# wlan-id 1 ● Enable 802.1X authentication on the specified WLAN. Hostname(config)# wlansec 1 Hostname(config-wlansec)# security rsn enable Hostname(config-wlansec)# security rsn ciphers aes enable Hostname(config-wlansec)# security rsn akm 802.1x enable Hostname(config-wlansec)# exit
Verification	Check the configuration of VLAN group 1.
	Hostname#show vlan-group 1 vlan-group id mode default-vlan vlan-list ---------- ---------- ---------- ---------- 1 dot1x 10 10-15

Common Errors

- A VLAN group with VLAN members is not created.
- The default VLAN is not contained in the VLAN group.

1.4.3 Configuring 802.1X Parameters

Configuration Effect

- Adjust 802.1X parameter configurations based on the actual network situation. For example, if the authentication server has poor performance, you can raise the authentication server timeout.

Notes

- 802.1X and RADIUS have separate server timeouts. By default, the authentication server timeout of 802.1X is 5 seconds while that of RADIUS is 15 seconds. In actual situations, ensure that the former is greater than the latter. You can run the **dot1x timeout server-timeout** command to adjust the authentication server timeout of 802.1X. For detailed configuration about the RADIUS server timeout, see the *Configuring RADIUS*.

Configuration Steps

Enabling Re-authentication

- (Optional) After re-authentication is enabled, the NAS can periodically re-authenticate online users.
- Enable re-authentication after 802.1X authentication is enabled on the NAS.

Command	**dot1x re-authentication**
Parameter Description	N/A
Defaults	Re-authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	You can run this command to periodically re-authenticate users.

Configuring the Re-authentication Interval

- (Optional) You can configure the re-authentication interval for users.
- Configure the re-authentication interval after 802.1X authentication is enabled on the NAS. The re-authentication interval takes effect only after re-authentication is enabled.

Command	**dot1x timeout re-authperiod** *period*
Parameter Description	*period*: Indicates the re-authentication interval in the unit of seconds.
Defaults	The default value is 3,600 seconds.
Command Mode	Global configuration mode
Usage Guide	Adjust the re-authentication interval as required.

Configuring the Interval of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates a longer interval of packet retransmission.
- Configure the interval of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout tx-period** *period*
Parameter Description	*period*: Indicates the interval of EAP-Request/Identity packet retransmission in the unit of seconds.
Defaults	The default value is 4 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Adjust the value based on how long the authentication client responds to the NAS's requests.

Configuring the Maximum Times of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x reauth-max** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Identity packet retransmission.
Defaults	The default value is 6.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. In the case of high-rate packet loss, increase this value so that the clients can easily receive packets from the NAS.

Configuring the Interval of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates a longer retransmission interval.
- Configure the interval of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout supp-timeout** *time*
Parameter Description	*time*: Indicates the interval of EAP-Request/Challenge packet transmission in the unit of seconds.
Defaults	The default value is 3 seconds for switches while 4 seconds for wireless devices.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

Configuring the Maximum Times of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x max-req** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Challenge packet retransmission in the unit of seconds.
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Optional. It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

Configuring the Authentication Server Timeout

- (Optional) A larger value indicates a longer authentication server timeout.
- Configure the authentication server timeout after 802.1X authentication is enabled on the NAS.

- The server timeout of RADIUS must be greater than that of 802.1X.

Command	**dot1x timeout server-timeout** *time*
Parameter Description	*time*: Indicates the authentication server timeout in the unit of seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value if the communication between the NAS and RADIUS server is unstable.

Configuring the Quiet Period after Authentication Fails

- (Optional) A larger value indicates a longer quiet period.
- Configure the quiet period after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout quiet-period** *time*
Parameter Description	*time*: Indicates the quiet period after authentication fails. The unit is second.
Defaults	The default value is 10 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value to prevent users from frequently initiating authentication to the RADIUS server, thereby reducing the load of the authentication server.

Specifying the Authentication Mode

- (Optional) Configure the mode for 802.1X authentication.
- Configure the authentication mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-mode** {**eap** | **chap** | **pap**}
Parameter Description	**eap**: Indicates EAP authentication. **chap**: Indicates CHAP authentication. **pap**: Indicates PAP authentication.
Defaults	The default value is **eap**.
Command Mode	Global configuration mode
Usage Guide	Select the authentication mode supported by Ruijie Supplicant and authentication server.

Configuring Connection Status Detection for Ruijie Supplicants

- (Optional) After this function is enabled, Ruijie suppliant disconnection will be detected in a timely manner, avoiding inaccurate accounting.
- The supplicant must be a Ruijie 802.1X authentication supplicant.
- Configure this function after 802.1X authentication is enabled.

Command	**dot1x client-probe enable**
Parameter	N/A

Description	
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	You are advised to enable this function when using the Ruijie supplicant.

Configuring a Detection Interval for Ruijie Supplicants

- (Optional) A greater value indicates a longer interval at which the supplicant sends heartbeat packets.
- Configure this function after 802.1X authentication is enabled.

Command	**dot1x probe-timer interval** *time*
Parameter Description	*time:* Indicates the interval at which the Ruijie supplicant sends heartbeat packets to the device. The value is expressed in seconds and the default value is 20.
Defaults	The default value is 20.
Command Mode	Global configuration mode
Usage Guide	The default value is recommended.

Configuring a Detection Timer for Ruijie Supplicants

- (Optional) A greater value indicates a longer interval at which the device identifies disconnection of the supplicant.
- Configure this function after 802.1X authentication is enabled.

Command	**dot1x probe-timer alive** *time*
Parameter Description	*time:* Indicates the interval in seconds at which the device identifies disconnection of the supplicant. The default is 250.
Defaults	The default value is 250.
Command Mode	Global configuration mode
Usage Guide	Optional. If the device does not receive any response packets from the online supplicant within the period defined by the detection timer, the device identifies the supplicant disconnection. The default value is recommended.

Verification

Run the **show dot1x** command to check whether parameter configurations take effect.

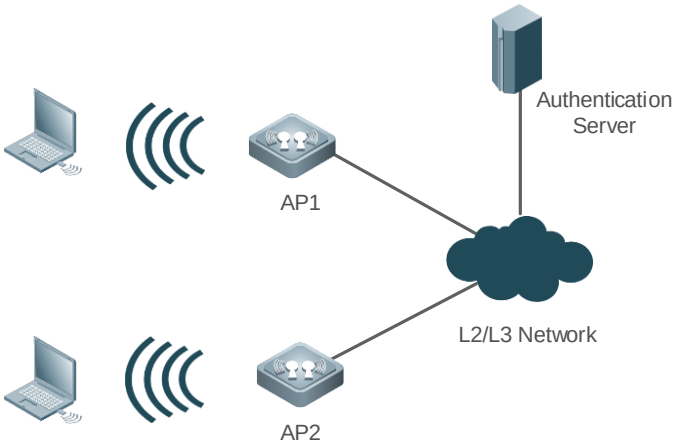
Configuration Example

Specifying the Authentication Mode

Scenario	The NAS is deployed in standalone mode.
Configuration Steps	Set the authentication mode to **chap**.
	Hostname(config)#dot1x auth-mode chap

Verification	Display the configurations. Hostname#show dot1x 802.1X basic information: 802.1X Status ..... enable Authentication Mode ..... chap Authorization mode ..... disable Total User Number ..... 0 (exclude dynamic user) Authenticated User Number ..... 0 (exclude dynamic user) Dynamic User Number ..... 0 Re-authentication ..... disable Re-authentication Period ..... 3600 seconds Re-authentication max ..... 3 times Quiet Period ..... 10 seconds Tx Period ..... 30 seconds Supplicant Timeout ..... 3 seconds Server Timeout ..... 5 seconds Maximum Request ..... 3 times Client Online Probe ..... disable Eapol Tag ..... disable 802.1x redirect ..... disable Private supplicant only ..... disable

Configuring Connection Status Detection for Ruijie Supplicants

Scenario Figure 1-4	
Configuration Steps	Enable connection status detection for Ruijie supplicants on the AP.
	Hostname(config)#dot1x client-probe enable
Verification	● Ruijie supplicants keep online by sending heartbeat packets periodically. ● Display the configuration.
	Hostname(config)#show dot1x

	802.1X basic information: 802.1X Status ..... enable Authentication Mode ..... chap Authorization mode ..... disable Total User Number ..... 0 (exclude dynamic user) Authenticated User Number ..... 0 (exclude dynamic user) Dynamic User Number ..... 0 Re-authentication ..... disable Re-authentication Period ..... 3600 seconds Re-authentication max ..... 3 times Quiet Period ..... 10 seconds Tx Period ..... 30 seconds Supplicant Timeout ..... 3 seconds Server Timeout ..... 5 seconds Maximum Request ..... 3 times Client Online Probe ..... enable Eapol Tag ..... disable 802.1x redirect ..... disable

Common Errors

- The server timeout is shorter than the RADIUS timeout.
- Connection status detection is configured for non-Ruijie supplicants.

1.4.4 Configuring MAB

Configuration Effect

- MAB uses the MAC address of an STA as the authentication account, eliminating the need to install a supplicant on the STA. MAB is applicable to dumb terminals, such as network printers.
- On WLANs, WLAN-based MAB is supported. If MAB is enabled, the NAS automatically associates the MAC address of an STA on the WLAN as the user name and password to initiate authentication to the authentication server.

Notes

- If MAB is enabled on a WLAN, set the WLAN security mode to OPEN.

Configuration Steps

↘ Enabling WLAN-based MAB

- Optional.
- Enable MAB on the WLAN connected to STAs.

Command	dot1x-mab
Parameter Description	N/A
Defaults	WLAN-based MAB is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	Run this command when STAs on a WLAN need to perform authentication using MAC addresses. This command applies only to wireless devices.

Enabling Uppercase Letters in MAB User Names

- Optional.
- Enable this function in global configuration mode.

Command	dot1x mab-username upper
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	By default, lowercase letters are used in the user name of MAB. After this function is enabled, uppercase letters are used in new user names of MAB to meet server requirements.

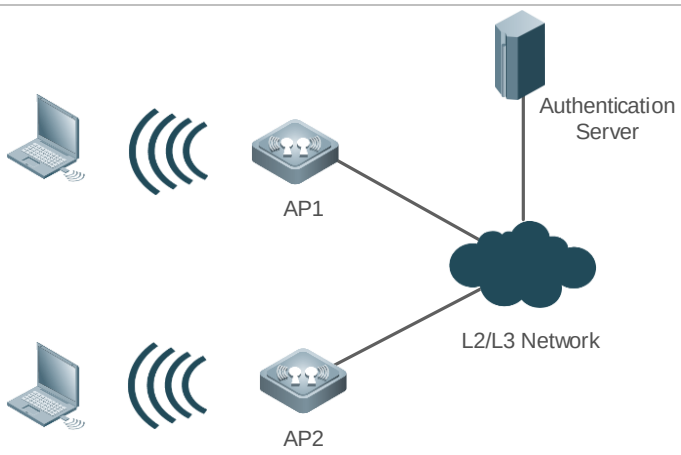
Verification

Check whether the dumb user can access the network. If yes, MAB takes effect. If no, MAB does not take effect.

- Check whether MAB functions are configured on the authentication server and NAS.
- Check whether dumb users with illegitimate MAC addresses cannot access the network.
- Check whether dumb users with illegitimate MAC addresses can access the network.

Configuration Example

Enabling WLAN-based MAB

Scenario Figure 4-6	

Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable WLAN-based MAB on the NAS. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	Hostname# configure terminal ruijie (config)# aaa new-model ruijie (config)# radius-server host 192.168.32.120 ruijie (config)# radius-server key ruijie Hostname(config)#wlansec 1 Hostname(config-wlansec)#dot1x-mab
Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username: 0023aeaa4286,password: 0023aeaa4286**. ● The STA fails to ping 192.168.32.120 before authentication. ● The STA connects to the NAS, the authentication succeeds, and the STA can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --- --- --- --- --- --- --- --- --- --- 16778217 0023aea... 0023.aeaa.4286 Gi0/1 2 Authenticated Idle Authed static 0days 0h 5m 8s

Common Errors

- The MAC account format is incorrect on the authentication server.

1.4.5 Configuring Extended Functions

Configuration Effect

- The multi-account function allows a user to switch its account upon re-authentication. In special scenarios such as Windows domain authentication, multiple authentications are required to access the domain and the user account changes during authentication. This function applies to these scenarios.
- 802.1X allows users to obtain IP addresses before accounting. In this manner, the IP address is carried during user accounting, meeting service requirements. After a user is authenticated and goes online, the

NAS can obtain the IP address of the user from the supplicant or through DHCP snooping, and then 802.1X server initiates an accounting request. To avoid the case in which the NAS does not initiate accounting for a long time due to failure to obtain the IP address of the authentication client, configure the IP detection timeout for this function. If the NAS does not obtain the IP address of the user within the configured time (5 minutes by default), it forces the user offline.

- 802.1X allows users to switch to the preset bypass WLAN when the RADIUS server is inaccessible. Survival WLANs are generally in OPEN mode and their services are unavailable by default. If 802.1X-based WLAN services are unavailable, enable this WLAN and disable WLAN-based 802.1X authentication so that users can switch to the bypass WLAN to properly access the network.
- 802.1X can be used with Web authentication. If Web authentication is enabled on an 802.1X-enabled WLAN, users perform 802.1X authentication only for encryption purposes. To access the network, they should also perform Web authentication. In this case, all air interface data of users is encrypted, enhancing security of user data.
- 802.1X provides prompts on syslog printing of user online/offline. You can adjust the online/offline syslog printing rate based on the user authentication rate to prevent high CPU utilization due to frequent syslog printing for a large number of users going online/offline.
- In the WLAN-based 802.1X authentication scenario, the NAS sends the authentication server SNMP traps to notify the online/offline status of users.
- In the WLAN-based 802.1X authentication scenario, traffic monitoring can be enabled on a WLAN. That is, if the traffic of an authenticated user is lower than the configured threshold within the specified period, the user will be forced offline so that the authentication server can perform accounting in a timely manner.
- The device enabled with 802.1X authentication can initiate an accounting request to the authentication server after receiving information about the STA installed with a supplicant. By doing this, the device can send information about the STA installed with a supplicant to the authentication server. To prevent a wired device's failure to obtain information of the STA installed with a supplicant for a long period of time, you can configure a timer. If the wired device does not obtain the STA information when the timer expires, the STA is disconnected.
- For wireless 802.1X authentication, WLAN-based domain authentication can be configured. That is, a domain name is configured on the WLAN. Then an authentication user without a domain name can be authenticated through the authentication server with the domain name.

Notes

- The multi-account function must be disabled if accounting is enabled. Otherwise, accounting may be inaccurate.
- IP-based accounting is not required in two situations:
  - IPv4 addresses and Ruijie Supplicant are deployed. This function is not required because Ruijie Supplicant can upload the IPv4 addresses of users.
  - Static IP addresses are deployed.

- It is recommended that the SSID of the bypass WLAN be different from that of the 802.1X-based WLAN so that the bypass WLAN services can be intuitively reflected. Moreover, when the WLAN needs to be switched due to server inaccessibility, users can manually switch the SSID once. Since the supplicant generally has a memory of the SSID, the SSID can be switched automatically in the future.
- Since 802.1X users are only for encryption purposes, the authorization, e.g., ACL assignment and rate limit assignment, to 802.1X users will not take effect. However, users need to pass Web authentication and be authorized to access the network.

Configuration Steps

Configuring the Virtual MAC Address as the Source MAC Address of 802.1X Authentication Packets

- (Optional) Configure this command if the Ruijie supplicant fails to identify the MAC address of the Ruijie device.
- Configure this function after enabling 802.1X authentication.

Command	dot1x pseudo source-mac
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Some Ruijie supplicants may fail to identify the Ruijie device through the MAC address of the eapol packet. Use this command to configure 00-1A-A9-17-FF-FF as the source MAC address of the eapol packet, thereby ensuring that the supplicant can identify the Ruijie device.

Enabling Multi-account Authentication with One MAC Address

- (Optional) Run the **dot1x multi-account enable** command to allow the same MAC address to be used by multiple accounts.
- Enable multi-account authentication with one MAC address after 802.1X authentication is enabled on the NAS.

Command	dot1x multi-account enable
Parameter Description	N/A
Defaults	Multi-account authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when multi-account authentication is required in 802.1X authentication, e.g. in the case of Windows domain authentication. In this case, the authentication client can directly use a new account to initiate authentication while the previous account is still online. Multi-account authentication is disabled by default.

Enabling IP-triggered Accounting

- (Optional) If IP-triggered accounting is enabled, the NAS sends an accounting request to the authentication server after obtaining the IP address of the user.

- Enable IP-triggered accounting after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct enable**
Parameter Description	N/A
Defaults	IP-triggered accounting is disabled by default.
Command Mode	Global configuration mode
Usage Guide	If both accounting and IP-triggered accounting are enabled, the NAS initiates accounting only after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address. If accounting is disabled but IP-triggered accounting is enabled, the NAS does not initiate accounting after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address within the timeout.

Configuring the Timeout of Obtaining IP Addresses After Authentication

- (Optional) Configure the timeout of obtaining IP addresses if IP-triggered accounting is enabled.
- Configure the IP address obtaining timeout after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct timeout** *time*
Parameter Description	*time:* Indicates the timeout in the unit of minutes.
Defaults	The default value is 5 minutes.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Configure this command when there is a need to change the IP address obtaining timeout after users pass authentication.

Configuring 802.1X Authentication for Encryption Only When802.1X and Web Authentication Are Both Enabled

- (Optional) If 802.1X and Web authentication is enabled meanwhile, 802.1X is used only for encryption.
- Enable this function after 802.1X authentication is enabled on the NAS.

Command	**dot1x encryption only**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	It is recommended to retain the default setting.

Limiting the Rate of Printing Online and Offline Logs

- (Optional) You can limit the syslog printing rate upon 802.1X users going online/offline.
- Enable the syslog printing rate limit after 802.1X authentication is enabled on the NAS.

Command	**dot1x logging rate-limit** *value*
Parameter	*value:* Indicates the syslog printing rate per second upon users going online/offline. The default value

Description	is 5 per second. 0 indicates no rate limit.
Defaults	The default value is 5 per second.
Command Mode	Global configuration mode
Usage Guide	Generally it is recommended to use the defaults. If a large number of users frequently go online/offline, reduce this rate.

Enabling SNMP Trap During Online and Offline

- (Optional) The **dot1x user-trap enable** command is used to control whether to send traps to the SNMP server when 802.1X users go online or offline.
- Enable SNMP trap after 802.1X authentication is enabled on the NAS.

Command	**dot1x user-trap enable**
Parameter Description	N/A
Defaults	SNMP trap is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This command applies only to wireless 802.1X authentication devices. Configure this command when the NAS should send online/offline traps to the SNMP server. You also need to enable trap on the SNMP server. For details, see the *Configuring SNMP*.

Enabling Traffic Detection

- (Optional) If traffic detection is enabled, 802.1X-authenticated users with traffic lower than the threshold in the detection period will be kicked off to avoid incorrect accounting.
- Enable traffic detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x offline-detect** [**interval** *val* | **flow** *num* | **interval** *val* **flow** *num*]
Parameter Description	*val*: Indicates the detection period. The default value is 8 hours. *num*: Indicates the traffic threshold. The default value is 0 KB.
Defaults	By default, traffic detection is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	This command applies only to wireless 802.1X authentication devices. Configure this command when the NAS needs to detect STAs offline in a timely manner to prevent incorrect accounting.

Configuring Filtering of Print Information

- Optional

Configure this function after 802.1X authentication is enabled.

Command	**dot1x dbg-filter** *H.H.H*
Parameter Description	*H.H.H*: Indicates the MAC address of a user whose debugging information needs to be output.
Defaults	Debugging information of all authentication users is printed by default.

Command Mode	Global configuration mode
Usage Guide	To identify a fault on a network involving numerous users, you can run this command to print debugging information of specified users. Avoid too much debugging information, which may affect device performance.

1.5 Monitoring

Clearing

⚠ Authentication user information can be cleared after 802.1X is disabled.

Description	Command
Clears 802.1X user information.	**clear dot1x user**
Restores the default 802.1X configuration.	**dot1x default**

Displaying

Description	Command
Displays the parameters and status of the RADIUS server.	**show radius server**
Displays 802.1X status and parameters.	**show dot1x**
Displays the list of hosts allowed for authentication.	**show dot1x auth-address-table**
Displays the active authentication status.	**show dot1x auto-req**
Displays the status and parameters of host probe.	**show dot1x probe-timer**
Displays of the information of authenticated users.	**show dot1x summary**
Displays the maximum times of EAP-Request/Challenge packet retransmission.	**show dot1x max-req**
Displays the information of controlled ports.	**show dot1x port-control**
Displays filtering of non-Ruijie supplicants.	**show dot1x private-supplicant-only**
Displays the re-authentication status.	**show dot1x re-authentication**
Displays the maximum times of EAP-Request/Identity packet retransmission.	**show dot1x reauth-max**

Displays the quiet period after authentication fails.	**show dot1x timeout quiet-period**
Displays the re-authentication interval.	**show dot1x timeout re-authperiod**
Displays the authentication server timeout.	**show dot1x timeout server-timeou**t
Displays the supplicant timeout.	**show dot1x timeout supp-timeout**
Displays the interval of EAP-Request/Identity packet retransmission.	**show dot1x timeout tx-period**
Displays user information based on the MAC address.	**show dot1x user mac**
Displays user information based on the user name.	**show dot1x user name**
Displays user information based on the VLAN group ID.	**show vlan-group** [*vlan-group-id*] **dot1x user name**

Debugging

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

Description	Command
Debugs AAA. (For details, see the *Configuring AAA*.)	**debug aaa**
Debugs RADIUS. (For details, see the *Configuring RADIUS*.)	**debug radius**
Debugs 802.1X events.	**debug dot1x event**
Debugs 802.1X packets.	**debug dot1x packet**
Debugs 802.1X state machine (STM).	**debug dot1x stm**
Debugs 802.1X internal communication.	**debug dot1x com**
Debugs 802.1X errors.	**debug dot1x error**

1 Configuring Web Authentication

1.1. Overview

1.1.1. Web Authentication

Web authentication controls user access to networks. It requires no authentication software on clients. Instead, users can perform authentication on common browsers.

When unauthenticated clients attempt to access the Internet using browsers, the network access server (NAS) forcibly redirects the browsers to a specified site pointing to a Web authentication server, also called a portal server. Users can access the services on the portal server before being authenticated, such as downloading security patches and reading notices. If a user wants to access network resources beyond the portal server, the user must get authenticated by the portal server through a browser.

Besides providing convenient authentication, the portal server performs Webpage interaction with browsers, providing personalized services, such as advertisements, notices, and business links on the authentication page.

Web Authentication Versions

There are three versions of Ruijie Web authentication, including First-Generation Web Authentication, Second-Generation Web Authentication, and Internal Portal (iPortal) Web Authentication. The Web authentication process varies with authentication versions. For details, see Section 1.3 "Features".

⚠ The three versions of Web authentication are highly divergent in features and configurations. It is recommended to read through the relevant chapters carefully before configuration.

⚠ Both Second-Generation Web Authentication and iPortal Web Authentication support local account authentication on the NAS. Because Remote Authentication Dial In User Service (RADIUS) authentication is more commonly used in reality, it is used as an example in the chapter "Applications".

⚠ The concept of "interface" varies with product types. The interfaces on wireless devices may represent a wireless local area network (WLAN). This document uses the unified term "interface" to include them. In application.

⚠ Web authentication supports user online traffic detection. For details, see the Configuring SCC.

⚠ Web authentication supports the authentication of domain names. That is, accounts can be authenticated in the format of user name@domain name. This requires enabling the domain-name-based authentication, authorization and accounting (AAA) service. For details, see the Configuring AAA.

Protocols and Standards

- HTTP: RFC1945 and RFC2068
- HTTPS: RFC2818
- SNMP: RFC1157 and RFC 2578
- RADIUS: RFC2865, RFC2866, and RFC3576

- For the standards related to MAC SMS authentication, see the CMCC WLAN Device Interface Standards V3.1.0_20130901 (MAC Address-Based Authentication Extension), Zhejiang CMCCWLAN Fast Authentication Scheme – Interface Standards V1.1-2011.3.22, and WLAN Fast MAC Address-Based SMS Authentication Scheme V1.1-2011.3.21.

1.2. Applications

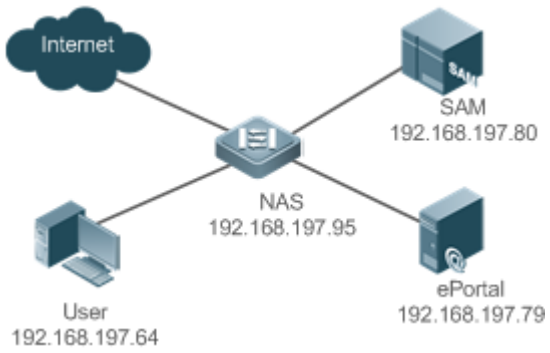
Application	Description
Basic Scenario of Web Authentication	Basic layer-2 authentication scenario, where a NAS, portal server, and RADIUS server constitute an authentication system which connects a client with the NAS through the layer-2 network.

1.2.1. Basic Scenario of Web Authentication

Scenario

- Deploy a Web authentication scheme on the NAS.
- The client connected to the NAS needs to pass Web authentication before accessing the Internet.

Figure 1-1 Networking Topology of Web Authentication



Remarks	Web authentication is applicable to both layer-2 and layer-3 networks. At layer 3, the source MAC address and VID of a packet are changed after it is routed, but the source IP address remains the same as the only identifier of a client. Therefore, the binding policy of Web authentication on layer-3 devices must adopt the IP-only binding mode. Here, layer-2 NAS is used as an example. RG-SAM program is installed on the RADIUS server. RG-ePortal program is installed on the portal server.

Deployment

- Enable Web authentication on the client-accessed interface or globally on the NAS.
- Configure the ePortal server and the communication key on the NAS (for only Ruijie First-Generation and Second-Generation Web Authentication).
- Configure the Simple Network Management Protocol (SNMP) communication parameters of the ePortal server on the NAS (for only Ruijie First-Generation and Second-Generation Web Authentication).

- Configure the consistent communication parameters on the ePortal server and SAM server (for only Ruijie First-Generation Web Authentication).
- Create user accounts on the SAM server.
- Configure AAA and method lists on the NAS (for only Ruijie Second-Generation and iPortal Web Authentication).
- Configure the IP address of the SAM server on the NAS (for only Ruijie Second-Generation and iPortal Web Authentication).
- Configure the names of the Web authentication method lists on the NAS (for only Ruijie Second-Generation and iPortal Web Authentication).

1.3. Features

Basic Concepts

First-Generation Web Authentication

The First-Generation Web Authentication should cooperate with the RG-ePortal software. The server installed with RG-ePortal provides a login page to submit user authentication information, and initiates an authentication request to the RADIUS server directly. After authentication succeeds, the NAS gets user information delivered through the SNMP protocol, and thereby controls user access permissions. Communication during Web authentication of this version depends on private SNMP nodes. Moreover, the ePortal server takes the place of the NAS in authentication and accounting, which relieves the NAS from service burden.

Second-Generation Web Authentication

Ruijie Second-Generation Web Authentication complies with the *CMCC WLAN Service Portal Specification*. The portal server is responsible only for Webpage interaction with users. The NAS interacts with the RADIUS server to implement authentication. The interaction between the portal server and the NAS complies with the *CMCC WLAN Service Portal Specification*. The portal server provides a login page for users to submit their information, and informs the NAS of user information through the portal protocols. The NAS completes authentication by interacting with the RADIUS server based on the user information, assigns access permissions to authenticated clients, and returns authentication results to the portal server.

The implementation process of Ruijie Second-Generation Web Authentication is mainly completed on the NAS. This raises a higher demand on the NAS's capability to handle heavy tasks. Meanwhile, the portal server is simplified. The standard *CMCC WLAN Service Portal Specification*, which gains highly industry support, enables various vendors to develop compatible products.

iPortal Web Authentication

In iPortal Web Authentication, the NAS integrates Webpage interaction of the portal server and partial authentication interaction of the RADIUS server. The NAS has a default authentication page suite. It can be customized according to the configuration described in this manual. Then, download the configured page suite to the storage medium of the NAS for effect.

Version Comparison

Authentication roles:

- Client: Its functions are the same among the three types of Web authentication.
- NAS: In First-Generation Web Authentication, the NAS implements only URL redirection and exchanges user login/logout notifications with the portal server. In Ruijie Second-Generation Web Authentication, the NAS is responsible for redirecting and authenticating users as well as notifying the portal server of authentication results. In Ruijie iPortal Web authentication, the NAS integrates multiple functions including the URL redirection, Webpage interaction, and authentication.
- Portal server: In Ruijie First-Generation Web Authentication, the portal server is responsible for interaction with clients through Webpages, authenticating users, and notifying the NAS of authentication results. In Ruijie Second-Generation Web Authentication, the portal server is responsible for interacting with clients through Webpages, notifying the NAS of users' authentication information, and receiving authentication results from the NAS. In Ruijie iPortal Web Authentication, the portal server is built into the NAS and provides simplified functions, mainly responsible for Web page interaction with clients.
- RADIUS server: Its functions are the same among the three types of Web authentication.

Authentication process:

- In Second-Generation Web Authentication, the authentication and accounting functions are transferred from the portal server to the NAS.
- Because authentication proceeds on the NAS, the second-generation NAS does not need to wait for the authentication results notified by the portal server as the first generation.
- iPortal Web Authentication simplifies and integrates the features of the first- and second- generation portal servers into the NAS.

Logout process:

- In First-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, or traffic detection or port status detection performed by the NAS. In Ruijie Second-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS. In Ruijie iPortal Web Authentication, a logout action may be triggered by the voluntary logout of a user through clicking the **Logout** button on the online page, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS.
- In Ruijie First-Generation Web Authentication, Accounting Stop packets are sent by the portal server. In Ruijie Second-Generation Web Authentication, Accounting Stop packets are sent by the NAS, the same as Ruijie iPortal Web Authentication.

The selection of the Web authentication versions depends on the type of the portal server in use.

Command parameters in this document may be shared by the three Web authentication versions or not. Read through this document carefully to avoid parameter misconfiguration that will affect Web authentication.

Overview

Feature	Description

Feature	Description
First-Generation Web Authentication	The portal server is deployed and supports only Ruijie First-Generation Web Authentication.
Second-Generation Web Authentication	The portal server is deployed and complies with the *CMCC WLAN Service Portal Specification*.
iPortal Web Authentication	The portal server is not deployed, and the NAS supports Webpage interaction.
MAC Address-Based SMS Authentication	An unauthenticated user is allowed to use the Internet after accessing the WLAN network. After the traffic used over the specified interval reaches the specified threshold, the authentication device sends a request to query the bound MAC address.
WiFiDog Web Authentication	An unauthenticated user will be redirected to the authentication page for authentication.
WeChat Web Authentication	After assessing the WLAN network, a mobile phone user will be redirected to the **Connect to Wi-Fi via WeChat** page through the browser. The user can enable the WeChat client for authentication with a tap on the link.

1.3.1. First-Generation Web Authentication

HTTP Interception

HTTP interception means the NAS intercepts to-be-forwarded HTTP packets. Such HTTP packets are initiated by the browsers of the clients connected to the NAS, but they are not destined for the NAS. For example, when a client attempts to visit the website www.google.com using the Internet Explorer, the NAS is expected to forward the HTTP request packets to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

After HTTP interception is successful, the NAS redirects the HTTP requests from the client to itself to establish a session between them. Then, the NAS pushes a Webpage to the client through HTTP redirection, which can be used for authentication, software downloading or other purposes.

You can specify the clients and destination interfaces to enable or disable HTTP interception for Web authentication. In general, HTTP requests from unauthenticated clients will be intercepted, and those from authenticated clients will not. HTTP interception is the foundation of Web authentication. Web authentication is automatically triggered once HTTP interception succeeds.

HTTP Redirection

According to HTTP protocols, after the NAS receives a HTTP GET or HEAD request packet from a client, a packet with 200 (Ok) status code is replied if it is able to provide the required resources, or a packet with 302 (Moved Temporarily) status code is returned if unable. Another URL is provided in the 302 packet. After receiving the packet, the client may resend a HTTP GET or HEAD request packet to the new URL for requesting resources. This process is called redirection.

HTTP redirection is an important procedure following HTTP interception in Web authentication. It takes the advantage of 302 status code defined in HTTP protocols. HTTP interception creates a session between the NAS and a client. The client sends HTTP GET or HEAD request packets (which should have been sent to another site) to the NAS. The NAS responds with a 302 packet with a specific redirection page. Thereby, the client resends the requests to the redirection page.

Because more and more application programs run HTTP protocols, the use of the 302 redirection packet may divert a large amount of HTTP traffic (not sent by browsers) to the portal server, which will affect network authentication. To address this problem, HTTP redirection technology on the NAS adopts noise reduction to replace the 302 packets with the **js** script.

Working Principle

Figure 1-1 shows the networking topology of Web authentication.

First-generation Webauth roles:

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.

2. NAS: Is an access-layer device in a network (for example, a wireless access point [AP] on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication.

3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, sends the information to the RADIUS server for authentication, and notifies the client and NAS of the authentication result. Figure 1-1 shows Ruijie ePortal server.

4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. The portal server extracts users' authentication account information from HTTP packets and initiates authentication requests to the RADIUS server through the RADIUS protocol. The RADIUS server returns the authentication result to the portal server through the RADIUS protocol. Figure 1-1 shows the RADIUS server installed with the RG-SAM program.

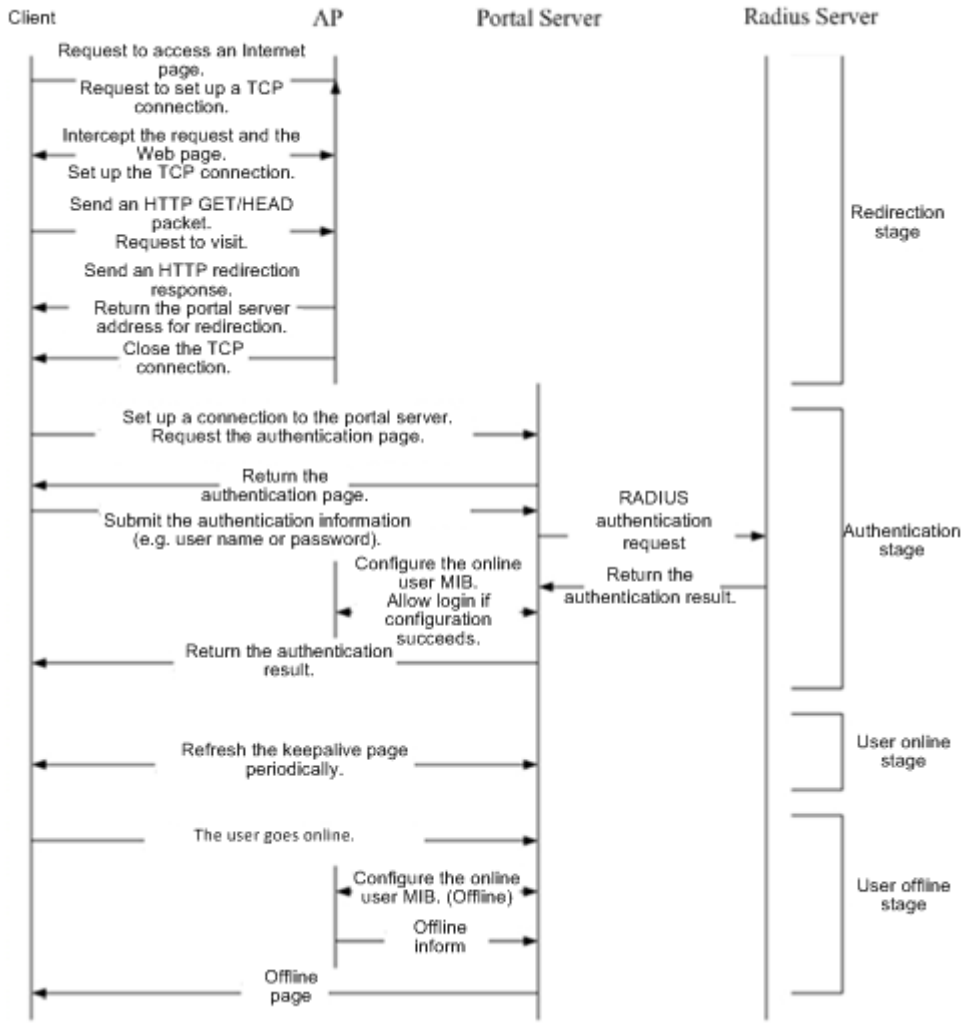
First-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.

1. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server and complete authentication.

2. After the user is authenticated, the portal server notifies the NAS that the client has passed authentication, and the NAS allows the client to access resources on the Internet.

Figure 1-2 Flowchart of Ruijie First-Generation Web Authentication



First-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. Scenario 1: The NAS detects a client to logout and informs the portal server. Then the portal server deletes the user information on the NAS through SNMP and displays a logout page to the client.

2. Scenario 2: The portal server detects a client to logout and informs the NAS through SNMP and displays a logout page to the client.

3. In the two scenarios, the portal server sends an Accounting Stop request to the RADIUS server and notifies the RADIUS server that the client has logged out.

Related Configuration

↘ Configuring the First-Generation Webauth Template

By default, the first-generation Webauth template is not configured.

Run the **web-auth template eportalv1** command in global configuration mode to create the first-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** {*string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling First-Generation Web Authentication

By default, First-Generation Web Authentication is disabled.

Run the **webauth** command in WLAN security configuration mode to enable the First-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Configuring the SNMP-Server Host

By default, the SNMP-server host and community string are not configured.

Run the **snmp-server host** {*ip-address* }**version 2c** {*community-string* } **web-auth** command in global configuration mode to configure the SNMP-server host and community string for Web authentication.

The SNMP-server host is configured to receive Inform/Trap packets of user logout.

Configuring the SNMP-Server Community String

By default, the SNMP-server community string is not configured.

Run the **snmp-server community** {*community-string*} **rw** command in global configuration mode to configure the SNMP-server community string.

The SNMP-server community string is configured to read/write user information from/to the NAS.

Enabling the SNMP Trap/Inform Function

By default, the SNMP Trap/Inform function is disabled.

Run the **snmp-server enable traps web-auth** command in global configuration mode to enable the SNMP Trap/Inform function.

The SNMP Trap/Inform function is configured to enable the NAS to inform the portal server of user logout.

1.3.2. Second-Generation Web Authentication

HTTP Interception

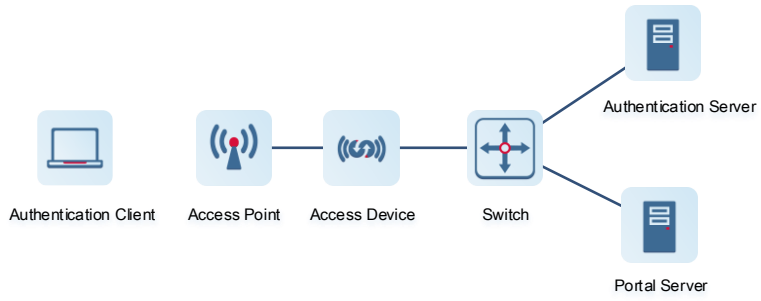
Same as the HTTP interception technology of Ruijie First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of Ruijie First-Generation Web Authentication.

Working Principle

Figure 1-1 External Portal Authentication System



Second-generation Webauth roles:

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.

2. NAS: An NAS is often a device at the access layer, for example, a wireless controller or an access point on a wireless network. An NAS needs to be enabled with external Portal authentication mode. An access device has the following functions:

(1) Obtains network access requests from the client.
(2) Pushes a redirection page to the client through HTTP redirection.
(3) Receives client information from the Portal server and initiates an authentication request to the authentication server.

(4) Allows or blocks the client's access to the Internet according to the authentication result and returns the result to the Portal server.

3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, transfers the information to the NAS, and displays the authentication result returned by the NAS to the user on a page. Figure 1-1 shows Ruijie ePortal server.

4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 1-1 shows the RADIUS server installed with the RG-SAM program.

Second-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.

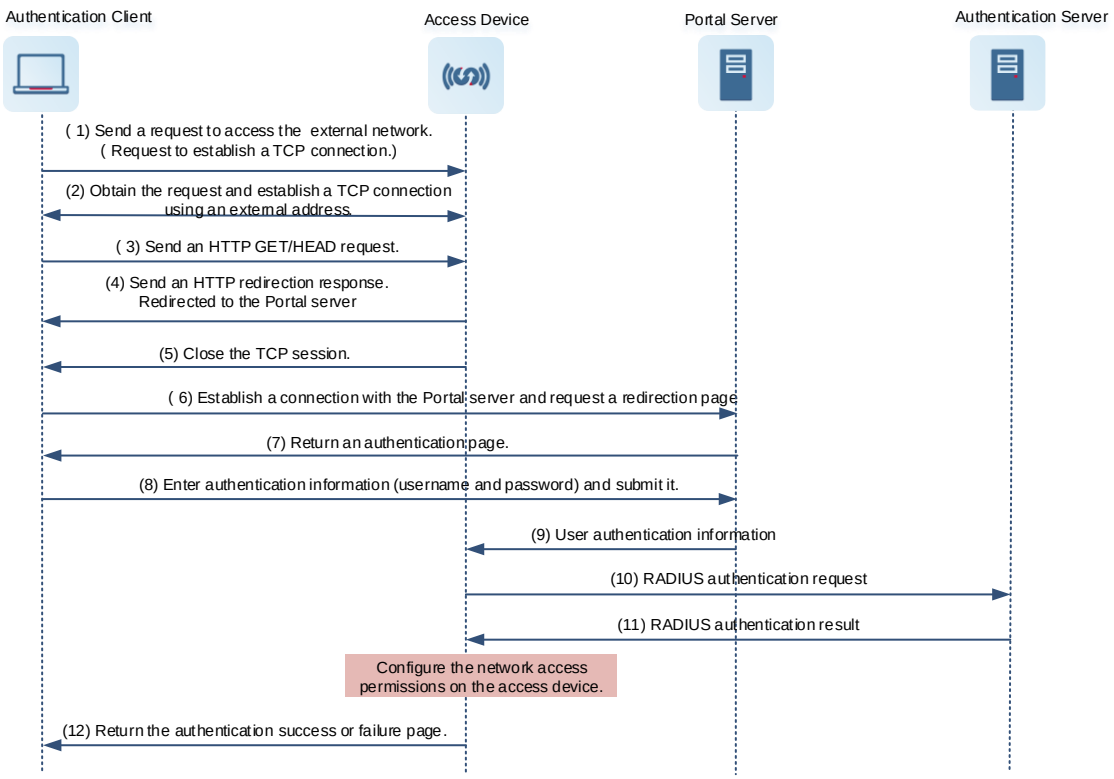
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.

3. The portal server sends the user authentication information to the NAS.

4. The NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.

5. The portal server displays the authentication result (success or failure) to the user on a page.

Figure 1-3 Flowchart of Ruijie Second-Generation Web Authentication



Second-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is

detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. When a user clicks the **Logout** button on the online page, the portal server notifies the NAS to get the user offline.

2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.

3. When the RADIUS server plans to force a client offline based on a certain policy, the NAS notifies the portal server to push a logout page to the client.

Related Configuration

Configuring the Second-Generation Webauth Template

By default, the second-generation Webauth template is not configured.

Run the **web-auth template** { **eportalv2** | *template-name* **v2** } command in global configuration mode to create a second-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** { *string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling Web Authentication

This function is disabled by default.

Run the **webauth** command to enable web authentication in WLAN security mode.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Ruijie Second-Generation Web Authentication relies on AAA. Enable AAA before you implement the former.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host is responsible for authenticating users.

Configuring an AAA Method List for Ruijie Second-Generation Web Authentication

By default, no AAA method list is configured for Ruijie Second-Generation Web Authentication.

Run the **aaa authentication web-auth** command in global configuration mode to configure an AAA method list for Ruijie Second-Generation Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

Configuring an AAA Method List for Ruijie Second-Generation Web Accounting

By default, no AAA method list is configured for Ruijie Second-Generation Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Ruijie Second-Generation Web Accounting.

The AAA method list for Web accounting is used for accounting interaction during the Webauth process.

Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

Specifying the UDP Port of the Portal Server

By default, UDP Port 50100 is used.

Run the **port** command in template configuration mode to specify the UDP port of the portal server.

The UDP port is specified for the portal server to communicate with the NAS.

1.3.3. iPortal Web Authentication

Working Principle

Internal Portal Authentication System

Figure 1-2 Internal Portal Authentication System



iPortal Webauth roles:

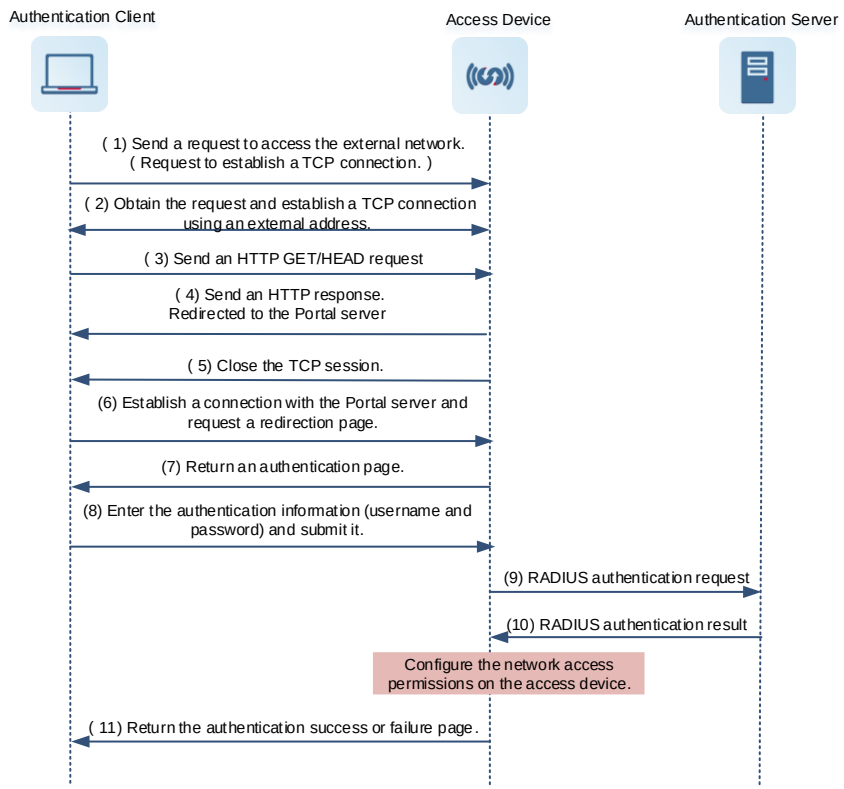
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.

2. NAS: Is an access-layer device in a network. It is directly connected to clients in wired or wireless networks and must be enabled with Ruijie iPortal Web Authentication. The NAS resolves the account information that clients enter on a Webpage and sends authentication requests to the RADIUS server. It determines whether clients can access the Internet according to authentication results and pushes the authentication results to the browsers.

3. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 1-1 shows the RADIUS server installed with the RG-SAM program.

Internal Portal Authentication Process

Figure 1-3 Internal Portal Authentication System



Procedure for a client to finish internal Portal authentication:

1. Before authentication, the access device obtains all HTTP requests from the unauthenticated client and redirects them to the internal Portal server. An authentication page will pop up on the client browser.

2. During authentication, the client enters authentication information such as username and password on the authentication page for interaction with the internal Portal server of the access device.

3. The internal Portal server sends authentication information of the client to the authentication module of the access device.

4. The authentication module processes authentication requests from the client, initiates an authentication request to the RADIUS server, and returns the authentication result to the internal Portal server.

5. The internal Portal server pushes the result page (authentication success or failure) to the client.

Related Configuration

↘ Configuring the iPortal Webauth Template

By default, the iPortal Webauth template is not configured.

Run the **web-auth template iportal** command in global configuration mode to create an iPortal Webauth template.

The template is used to configure authentication-related parameters on the iPortal server.

↘ Customizing a Page Suite

By default, the factory file package is used.

Run the **page-suite** command in template configuration mode to specify the use of a page suite.

Before you specify the use of a page suite, download it to the flash memory.

Configuring an Advertisement Push Method and URL

The advertisement is pushed after authentication by default.

Run the **login-popup** *url* command to configure the advertisement URL pushed before authentication in template configuration mode. Run the **online-popup** *url* command to configure the advertisement URL pushed after authentication in template configuration mode.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Enabling Ruijie iPortal Web Authentication

By default, Ruijie iPortal Web Authentication is disabled.

Run the **webauth** command in WLAN security configuration mode to enable iPortal Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Ruijie iPortal Web Authentication relies on AAA. Enable AAA before you implement Web authentication.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host in Web authentication is responsible for authenticating users.

Configuring an AAA Method List for Ruijie iPortal Web Authentication

By default, no AAA method list is configured for Ruijie iPortal Web Authentication.

Run the **aaa authentication iportal** command in global configuration mode to configure an AAA method list for Ruijie iPortal Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

Configuring an AAA Method List for Ruijie iPortal Web Accounting

By default, no AAA method list is configured for Ruijie iPortal Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Ruijie iPortal Web Accounting.

The AAA accounting method list is used for accounting interaction during the Webauth process.

↘ Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

↘ Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

1.3.4. MAC Address-Based SMS Authentication

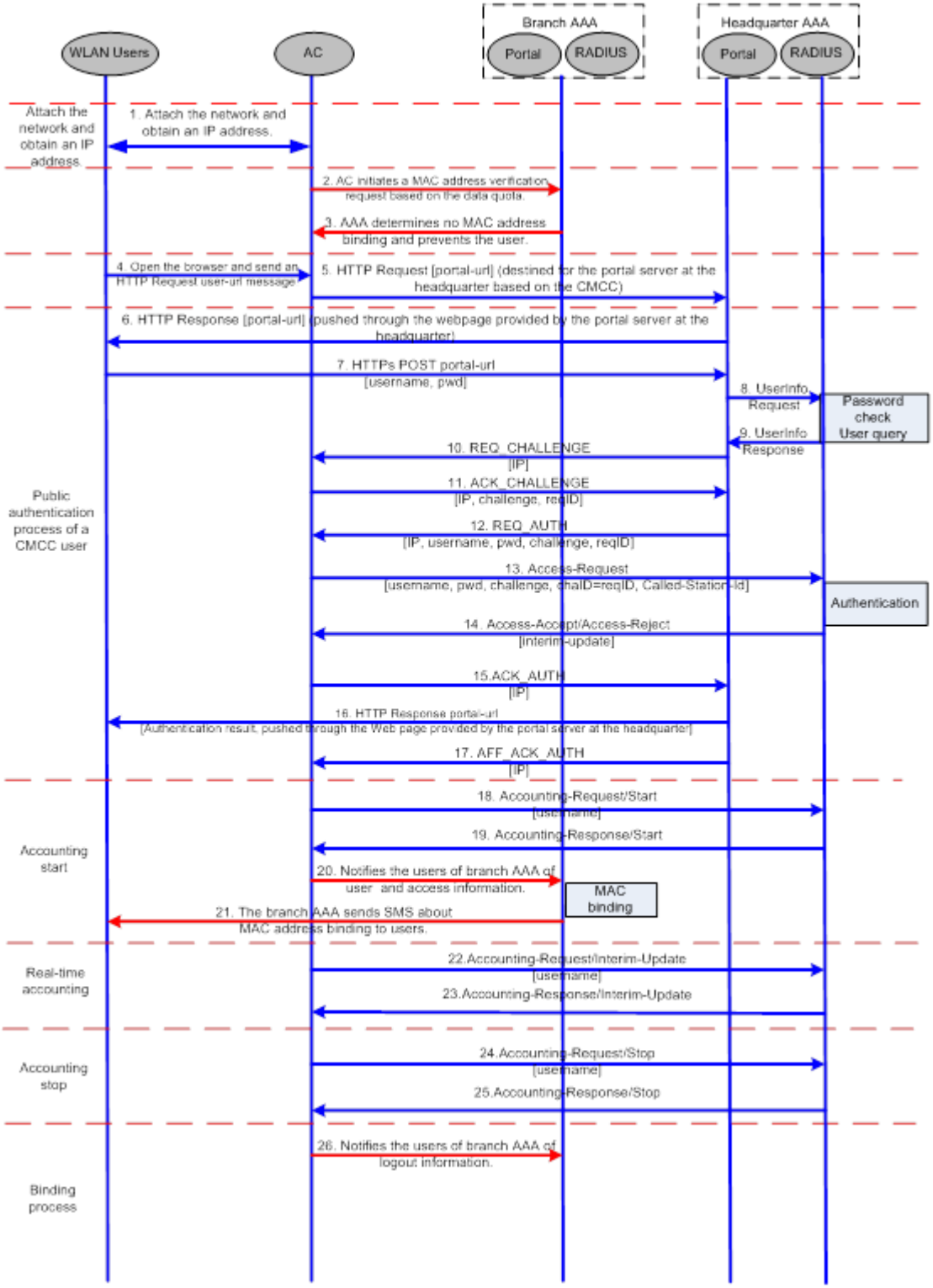
Working Principle

After an STA is associated with an SSID enabled with MAC address-based SMS authentication, the STA obtains an IP address through the Dynamic Host Configuration Protocol (DHCP). Then the STA is allowed to access the Internet. When the STA uses up the traffic allowed during a time period, the access controller (AC) initiates a MAC address binding query to the bound portal server. If the STA is bound with a MAC address, the portal server sends an authentication request. If the STA is not bound with a MAC address, the STA needs to re-perform authentication on the portal server before accessing the Internet.

↘ SMS Authentication Process for Unbound STAs

The following figure shows the process where an STA not bound with a MAC address associates the SSID enabled with MAC address-based SMS authentication to access the Internet. Compared with Ruijie Second-Generation Web Authentication, MAC address-based SMS authentication is added with the procedures of querying MAC address binding and notifying the bound portal server of user login/logout. The rest of the process is the same. If the STA selects the **Bind** check box when performing authentication on the portal server, the portal server will bind the STA with a MAC address. Next time the STA can access the Internet directly.

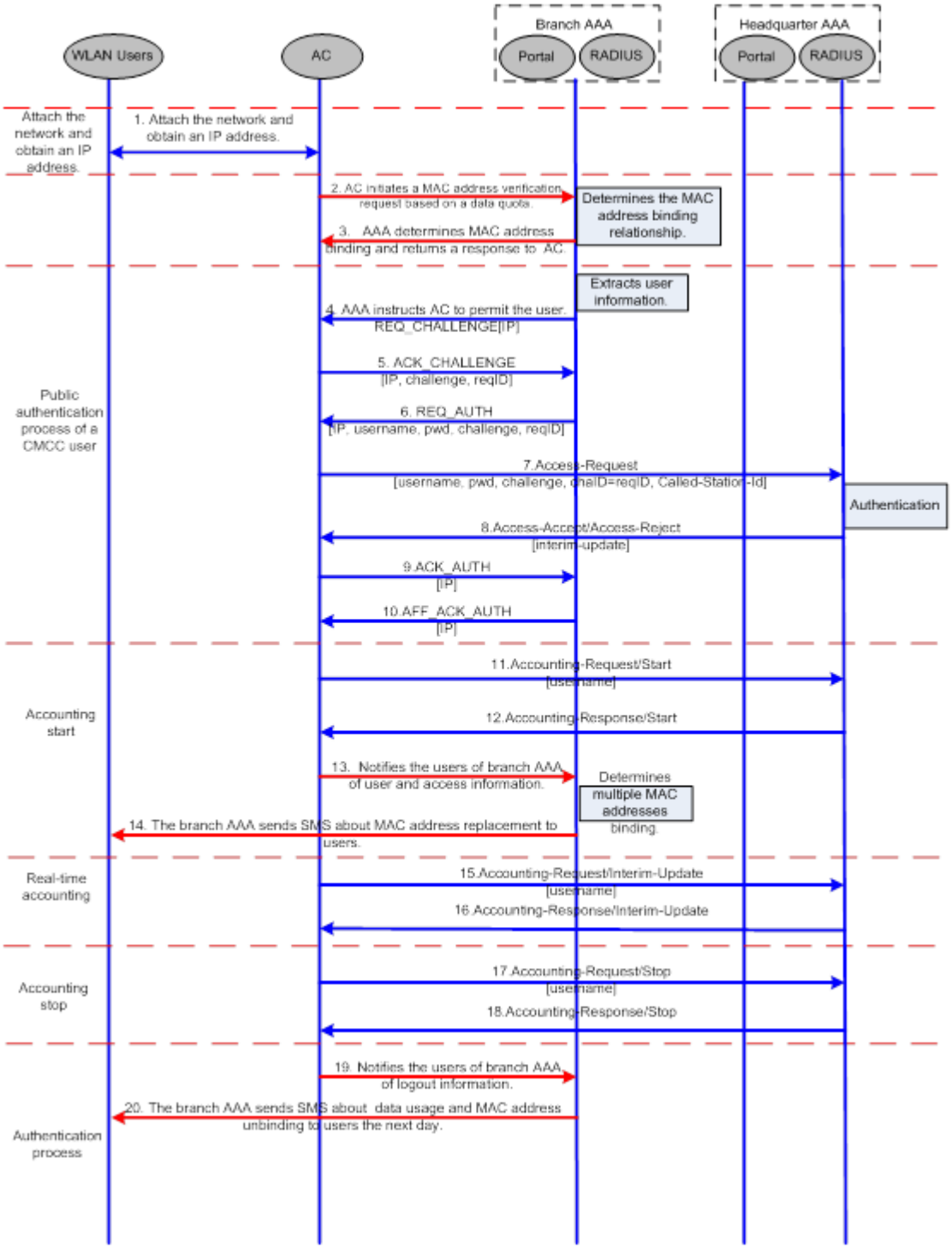
Figure 1-4 Flowchart of SMS Authentication for Unbound STAs



↘ SMS Authentication Process for Bound STAs

After an STA is bound with a MAC address, the user does not need to open the browser to perform authentication for Internet access. Network access is automatically completed after the STA is associated with a network, which greatly facilitates wireless network access.

Figure 1-5 Flowchart of SMS Authentication for Bound STAs



1.3.5. WiFiDog Web Authentication

HTTP Interception

Same as the HTTP interception technology of First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of First-Generation Web Authentication.

Working Principle

The networking topology of WiFiDog Web authentication is the same as shown in Figure 1-1.

Roles involved in WiFiDog Web authentication:

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.

2. NAS: Is an access-layer device in a network (for example, an AP on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication. The NAS controls users' Internet access permissions, receives the token check requests or Internet access requests from authentication clients, and initiates identity check to the portal server.

3. Portal server: Provides a Web page for Web authentication and related operations. The portal server receives the HTTP-based authentication requests from authentication clients and extracts account information from the requests. When authentication is complete in the background, the authentication clients forward the authentication results to the NAS. The NAS redirects the authentication clients to a Webpage provided by the portal server.

Main process of WiFiDog Web authentication:

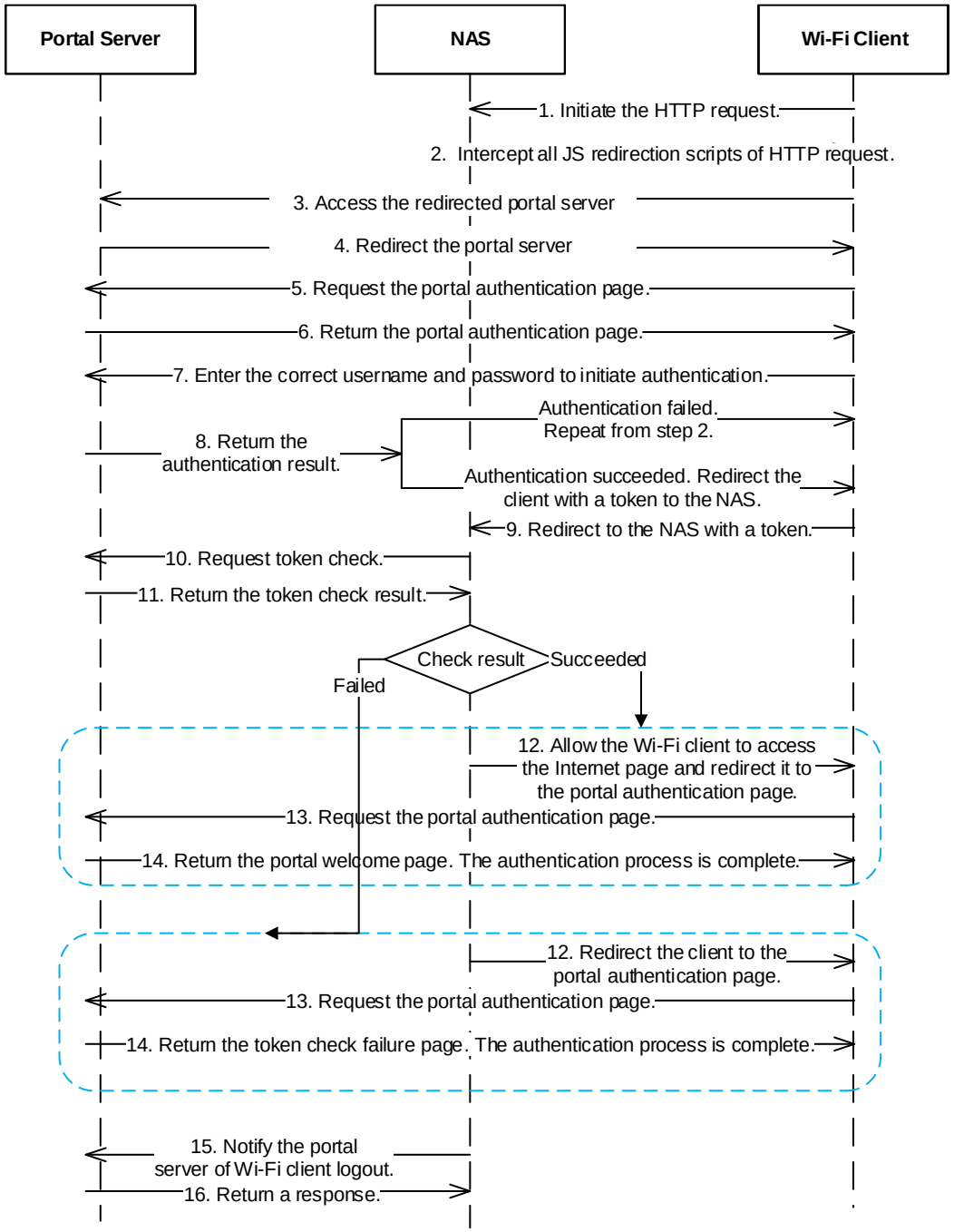
1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.

2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.

3. The portal server checks the validity of the client information in the background. If authentication fails, the portal server displays the failed authentication result to the client on a Web page. If authentication is successful, the portal server redirects the client to the NAS.

4. After receiving a request from the client, the NAS initiates check to the portal server. The NAS redirects the client to a Webpage provided by the portal server based on the check result.

Figure 1-6 Flowchart of WiFiDog Web Authentication



Client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page.

1. When a client clicks the **Logout** button, a logout request is sent to the portal server and NAS. (The logout request to the portal server and NAS may not be simultaneous, depending on the capability of the portal server.)

2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.

Related Configuration

Configuring a WiFiDog Webauth Template

By default, the WiFiDog Webauth template is not configured.

Run the **web-auth template** { **wifidog** |*template-name* **wifidog** } command in global configuration mode to create a WiFiDog Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** *url-string* command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Configuring the IP Address of the NAS

By default, the IP address of the NAS is not configured.

Run the **nas-ip** { *ip-address*} command in template configuration mode to configure the IP address of the NAS.

Ensure that the configured IP address is accessible by clients.

Configuring a Gateway ID

By default, the gateway ID is the serial number of the device. In the case of hot standby or Virtual Access Point (VAC), the gateway ID is required, which can be the MAC address of a member device.

Run the **gateway-id** { *string* } command to configure this function in template configuration mode.

This parameter is required by WiFiDog interactive packets. The command is open to a third-party Portal.

Enabling Web Authentication

This function is disabled by default.

Run the **webauth** command to enable web authentication in the WLAN security mode.

1.3.6. WeChat Web Authentication

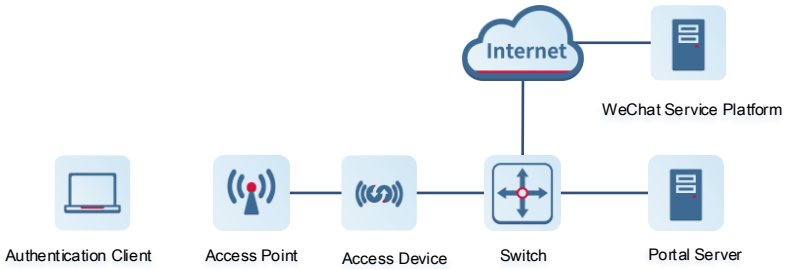
WeChat is an application that provides cross-platform instant messaging for access terminals, including iPhone, iPad, Android, and PC. The WeChat public platform establishes a direct communication platform between business owners and end users through official accounts. WeChat authentication is an authentication method for quickly connecting to Wi-Fi. By guiding mobile terminals to follow WeChat official accounts, business owners

tailor official accounts to specific needs, realize online and offline interoperability, and increase user stickiness. WeChat authentication is also a special Portal authentication. After business owners enable this authentication, mobile terminals do not need to enter complex passwords. By scanning the QR code of the official account, mobile terminals are redirected to the authentication wizard page provided by the Portal server for real-name authentication, ensuring secure access to the Internet.

Working Principle

WeChat authentication System

Figure 1-4 WeChat Authentication System



- Authentication Client (STA)

An authentication client can be a PC, iPhone, iPad, or Android-based terminal installed with WeChat. It is the initiator of WeChat authentication, and is often a regular customer in a shopping mall or a floating customer at the offline site.

- Access Device (AC or AP)

An access device can be an AC or AP on the wireless network. The access network needs to be enabled with web authentication in WeChat authentication mode. In the WeChat authentication system, the access device takes the following roles:

Before authentication, the access device obtains external HTTP requests from authentication clients and redirects the requests to the Portal server.

During authentication, the authentication client, access device, and Portal server implement authentication on clients through HTTP.

After authentication, the access device allows or denies the client's access to the Internet and returns the result page to the client.

- Portal Server

A Portal server is responsible for receiving authentication requests from the client, providing the WeChat authentication page, and exchanging authentication information with the access device. If WeChat authentication is used for WLAN access authentication, the Portal server is often a Ruijie-developed RG-MCP or RG-MACC server.

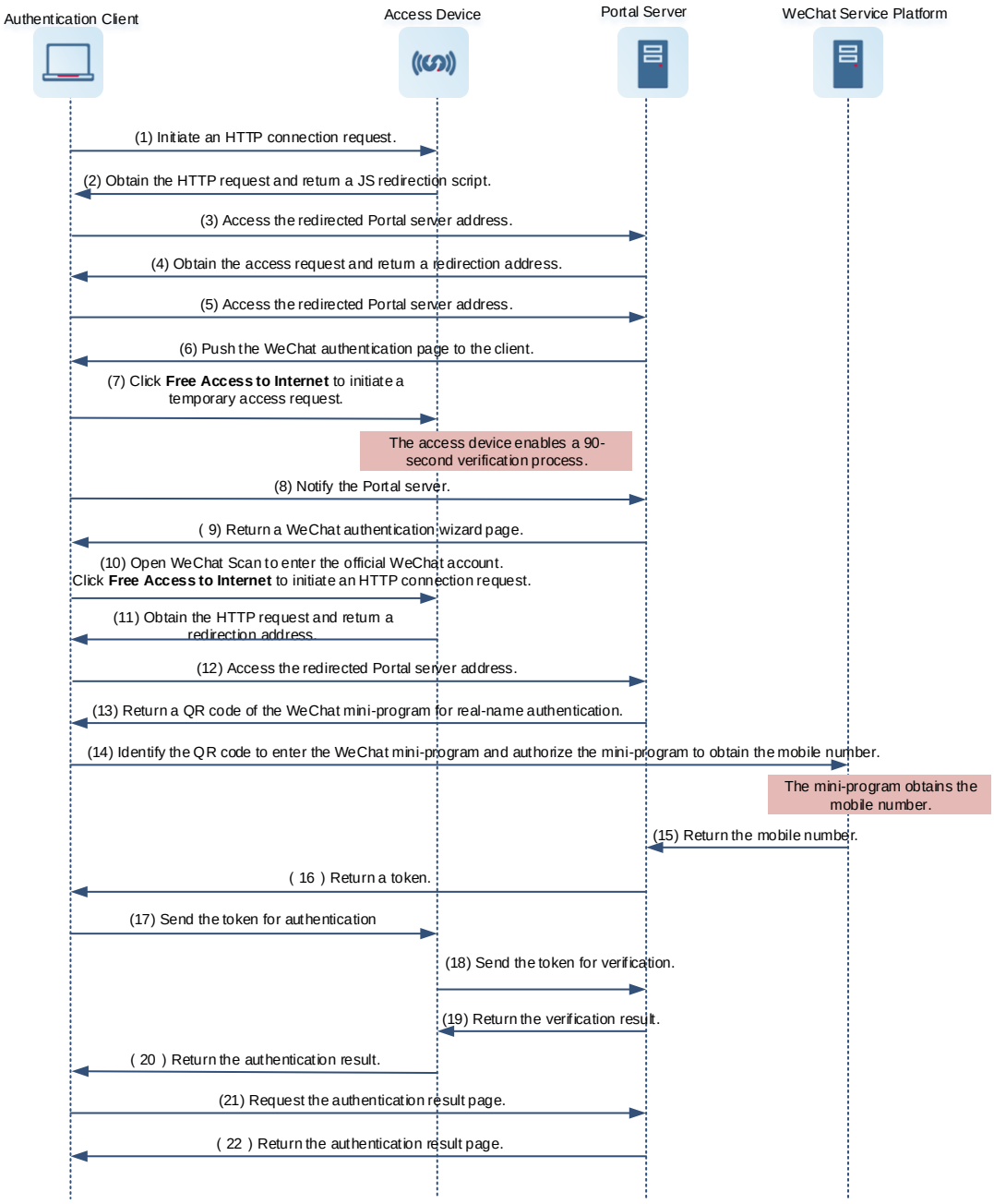
WeChat Service Platform

The WeChat service platform provides a variety of services during WeChat authentication process, such as WeChat official account service, WeChat mini-program service, and WeChat scan service. During WeChat authentication process, the authentication client scans the QR code of the business owner to access the WeChat

official account. The client authorizes the WeChat mini-program developed by Ruijie networks to obtain the mobile number of the client from the mini-program server for real-name authentication.

WeChat Authentication Process

Figure 1-5 WeChat Authentication Flowchart



WeChat authentication involves the following steps:

1. The authentication client connects to the Wi-Fi network enabled with WeChat authentication and initiates an HTTP connection request when accessing the Internet through a browser.
2. The access device obtains the HTTP request from the client and redirects it to the Portal server.

3. The client accesses the redirection URL and the Portal server pushes the WeChat authentication page to the client.
4. The client triggers the request for a 90-second verification process by clicking on **Free Access to Internet** and notifies the Portal server.
5. The access device enables the 90-second verification process after receiving the request from the client.
6. After receiving the notification from the client, the Portal server sends the WeChat authentication wizard page to the client for subsequent WeChat authentication.
7. The client enters the WeChat client homepage through the wizard page, opens WeChat scan, and scans the WeChat official account.
8. By clicking on **Free Access to Internet** in the official account, the client initiates an HTTP connection request.
9. The access device obtains the HTTP request and redirects it to the Portal server again. The Portal server returns the QR code of a WeChat mini-program for real-name authentication.
10. The client enters the WeChat mini-program by scanning the QR code and authorizes the WeChat mini-program to obtain the mobile number of the client.
11. The WeChat mini-program obtains the client's mobile number and returns it to the Portal server.
12. The Portal server obtains basic information about the client and returns an authentication token to the client.
13. The client sends the authentication token to the access device.
14. The access device sends the authentication token to the Portal server.
15. After receiving the authentication token, the Portal server identifies the client validity and returns a token verification result to the access device.
16. The access device configures the 90-second verification process according to the authentication result and returns the authentication result to the client.
17. The client requests the authentication result page from the Portal server.
18. The Portal server returns the authentication result page to the client.

Related Configuration

↘ Configuring a WeChat Webauth Template

By default, the WeChat Webauth template is not configured.

Run the **web-auth template** {**wechat** |*template-name* **wechat** } command in global configuration mode to create a WeChat Webauth template.

The template is used to implement Web authentication.

↘ Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

↘ Configuring the WeChat Webauth URL

By default, no WeChat Webauth URL is configured.

Run the **service-url** {*url-string* } command in template configuration mode to configure the WeChat Webauth URL.

The URL address is used for the communication between the NAS and portal server.

The URL can contain a domain name for interconnection with a MACC server. Ensure that only one IP address corresponding to the domain name is resolved. The protocol name will be removed automatically from the domain name during configuration. The device supports only HTTP URL resolution.

Run the **service_url** command to configure a domain name. The server IP address in the template will be overwritten by the IP address resolved from the domain name.

Configuring a Portal Server URL

By default, the Portal server URL is the SMS authentication redirection URL when both WeChat and SMS authentication are enabled.

Run the **url** { *url-string* } command to configure the Portal server URL in template configuration mode.

The URL is the SMS authentication redirection URL when both WeChat and SMS authentication are enabled.

Configuring the IP Address of the NAS

By default, the IP address of the NAS is not configured.

Run the **nas-ip** *ip-address* command in template configuration mode to configure the IP address of the NAS.

Ensure that the configured IP address is accessible by users and must not be configured as a authentication-free address.

Configuring the Portal Communication Key

By default, no encryption key is configured.

Run the **key** {*key-string*} command in template configuration mode to configure an encryption key used for communicating with the portal server.

The encryption key is used to encrypt user authentication information and must be consistent with the key configured on the portal server.

Enabling Web Authentication

By default, Web authentication is disabled.

Run the **web-auth portal** { **wechat** | *template-name* **wechat** } command in WLAN security configuration mode and **webauth** command to enable Web authentication control on the STA-connected port.

After Web authentication is enabled, the unauthenticated STAs connecting to the port will be redirected to a one-click Internet access page provided by the portal server, and the unauthenticated PCs connecting to the port will be redirected to a QR code page.

Enabling the Collective Escape Function

By default, the collective escape function is disabled.

Run the **web-auth wechat-escape interval** *minutes* command to configure this function in global configuration mode or WLAN security configuration mode.

The configuration in the WLAN security configuration mode prevails. If there is no configuration in the WLAN security configuration mode, the configuration in global configuration mode takes effect.

After the function is configured, the device starts counting single escape users. If the number of single escape users reaches the threshold (specified by **times** *count*) within a certain interval (specified by **interval** *minutes*), the device starts collective escape and all users who gain access later are permitted to pass without authentication.

To cancel collective escape, run the **web-auth wechat-escape recover** command in global configuration mode to restore the single escape state.

↘ Configuring Server Detection

By default, server detection is disabled.

Run the **web-auth wechat-check interval** *minutes* command in global configuration mode to enable server detection.

After the function is configured, the device detects the server. If it fails to receive the serve response or the response is unavailable within a certain interval (specified by **interval** *minutes*) and the collective escape function is configured on the device, all users who gain access later are permitted to pass without authentication.

To cancel server detection, run the **no web-auth wechat-check** command in global configuration mode.

1.4. Configuration

Configuration	Description and Command	
Configuring First-Generation Web Authentication	⚠ (Mandatory) It is used to set the basic parameters of Ruijie First-Generation Web Authentication.	
	web-auth template eportalv1	Configures the first-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url *url-string*	Configures the Webauth URL of the portal server.
	web-auth portal key *key-string*	Configures the Webauth communication key.
	snmp-server community { *community-string* } **rw**	Configures the SNMP-server community string.
	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	Configures the SNMP-server host.
	snmp-server enable traps web-auth	Enables the SNMP-server Trap/Inform function.
	webauth	Enables First-Generation Web Authentication on an interface.

Configuration	Description and Command	
Configuring Second-Generation Web Authentication	⚠ (Mandatory) It is used to set the basic parameters of Ruijie Second-Generation Web Authentication.	
	aaa new-model	Enables AAA.
	radius-server host { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *time*]] [**key** [**0** | **7**] *text-string*]	Configures the RADIUS-server host and communication key.
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Web authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Web Accounting. (RADIUS accounting is implemented.)
	web-auth template{**eportalv2** |*portal-name***v2**}	Configures a second-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url *url-string*	Configures the Webauth URL of the portal server.
	web-auth portal key *key-string*	Configures the Webauth communication key.
	webauth	Enables Second-Generation Web Authentication on an interface.
Configuring iPortal Web Authentication	⚠ (Mandatory) It is used to set the basic parameters of Ruijie iPortal Web authentication.	
	aaa new-model	Enables AAA.
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	Configures the RADIUS-server host and communication key.
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Ruijie iPortal Web Authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Ruijie iPortal Web Accounting. (RADIUS accounting is implemented.)
	web-auth template iportal	Configures the iPortal Web-auth template.
	webauth	Enables Ruijie iPortal Web Authentication on an interface.

Configuration	Description and Command	
Configuring WiFiDog Authentication	(Mandatory) It is used to set the basic parameters of MAC address-based SMS authentication.	
	aaa new-model	Enables AAA.
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	Configures the RADIUS-server host and communication key.
	web-auth template eportalv2	Configures a second-generation Webauth template.
	web-auth sms-flow interval *interval* **threshold** *flows*	Configures the detection interval and traffic threshold for MAC address-based SMS authentication.
	web-auth bind-portal *string* **[type { group-spec | local-spec}]**	Configures the portal server bound for MAC address-based SMS authentication.
	web-auth winterface *string*	Sets the **winterface** field in the redirected URL.
	web-auth wlan-ac-ip *ipv4*	Sets the **ACIP** field in the redirection URL.
Configuring MAC Address-Based SMS Authentication	(Mandatory) It is used to set the basic parameters of WiFiDog authentication.	
	web-auth template wifidog	Configures a WiFiDog authentication template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url *url-string*	Configures the Webauth URL of the portal server.
	nas-ip { *ip-address* }	Configures the IP address of the NAS.
	web-auth portal wifidog	Specifies a WiFiDog authentication template.
	webauth	Enables Web authentication.
Configuring WeChat Web Authentication	(Mandatory) It is used to set the basic parameters of WeChat authentication.	
	web-auth template { **wechat** | (*portal-name* **wechat**)}	Configures a WeChat Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	service-url { *url-string* }	Configures the WeChat Webauth URL.
	key { *key-string* }	Configures the portal communication key.
	web-auth portal wechat	Specifies a WeChat Webauth template.
	webauth	Enables Web authentication.

Configuration	Description and Command	
Specifying an Authentication Method List	(Optional) It is used to specify an AAA authentication method list in template configuration mode. The name of the method list must be correctly specified.	
	authentication { *mlist-name* }	Specifies an AAA authentication method list(only for Ruijie Second-Generation Web Authentication and Ruijie iPortal Web Authentication.)
Specifying an Accounting Method List	(Optional) It is used to specify an AAA accounting method in template configuration mode. The name of the method list must be correctly specified.	
	accounting { *mlist-name* }	Specifies an AAA accounting method list(only for Ruijie Second-Generation Web Authentication and Ruijie iPortal Web Authentication.)
Configuring the Communication Port of the Portal Server	(Optional) It is used to specify the UDP port of the portal server in template configuration mode. The configured port number must be consistent with that on the RADIUS server.	
	port { *port-num* }	Configures the communication port of the portal server.
Specifying the Webauth Binding Mode	(Optional) It is used to specify the entry binding mode in template configuration mode.	
	bindmode ip-mac-mode	Specifies the template binding mode.
Customizing a Page Suite	(Optional) It is used to configure the page suite used by Ruijie iPortal Web Authentication for a template.	
	page-suite *file-name*	Customizes a page suite for Ruijie iPortal Web Authentication.
Configuring the Advertisement Pushing Mode	(Optional) It is used to configure an iPortal Webauth advertisement URL in template configuration mode.	
	login-popup *url*	Configures a URL popping up before authentication, which is also the login popup URL.
	online-popup *url*	Configures a URL popping up after successful authentication.
Configuring a Custom URL	(Optional) It is used to configure the redirection URL format for a template.	

Configuration	Description and Command	
Format	**fmt custom encry** { [**none | md5 | des | des_ecb | des_ecb3**] } { [**user-ip** *userip-str*] [**user-mac** *usermac-str* **mac-format [dot | line | none | 5colon]**] [**user-vid** *uservid-str*] [**user-id userid-str**] [**nas-ip** *nasip-str*] [**nas-id** nasid-str **] [nas-id2** *nasid2-str* **]** [**ac-name** *acname-str*] [**ap-mac** *apmac-str* **mac-format [dot | line | none | 5colon]**] [**url** *url-str*] [**ssid** *ssid-str*] [**port** *port-str*] [**ac-serialno** *ac-sno-str*] [**ap-serialno** *ap-sno-str*] [**additional** *extern-str*] }	Configures the format of the Webauth URL.
Configuring the Redirection HTTP Port	(Optional) It is used to configure the TCP interception port for redirection, so that the packets on the specified port can be redirected when interception is enabled.	
	http redirect port *port-num*	Configures the redirection TCP port.
Configuring Rate Limit Webauth Logging	(Optional) It is used to configure the syslog function in Web authentication.	
	web-auth logging enable *num*	Configures the rate limit Webauth logging.
Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients	(Optional) It is used to adjust the HTTP session limit. The limit value needs to be increased when there are many sessions in the background.	
	http redirect session-limit { *session-num* } [**port** *port-session-num*]	Configures the maximum number of HTTP sessions for unauthenticated clients.
Configuring the HTTP Redirection Timeout	(Optional) It is used to modify the timeout period for redirection connections. The timeout needs to be increased to complete redirection when the network condition is bad.	
	http redirect timeout *seconds*	Configures the HTTP redirection timeout.
Configuring the Authentication-Free Network Resource	(Optional) It is used to permit the specified addresses to pass.	
	http redirect direct-site { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp** | *port-number*]}	Configures the address of the network exempt from authentication.
Configuring the Authentication-Free ARP Resource Range	(Optional) It is used to permit the ARP of the specified addresses to pass. The gateway ARP must be permitted to pass when ARP check is enabled.	
	http redirect direct-arp { *ip-address* [*ip-mask*] }	Configures the authentication-free ARP resource.

Configuration	Description and Command	
Configuring an Authentication-Free Address Range	(Optional) It is used to exempt clients from authentication when accessing the Internet.	
	web-auth direct-host { *ipv4-address* [*ip-mask*] [**arp**] } [**port** *interface-name*]	Configures the range of the IP addresses of clients free from authentication.
Configuring the Interval for Updating Online User Information	(Optional) It is used to configure the interval for updating online user information.	
	web-auth update-interval *{ seconds }*	Configures the interval for updating online user information.
Configuring Portal Detection	(Optional) It is used to detect the availability of the portal server. If it is not available, the services are switched to the standby portal server. This function must be used together with portal standby function.	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries**]**	Configures the portal server detection interval, timeout period, and timeout retransmission times.
	web-auth ping [**interval** *minutes* | **retry** *times*]	Configures the ping detection interval and timeout retransmission times.
Configuring Portal Escape	(Optional) It is used to allow new clients to access the Internet without authentication when the portal server is not available.	
	web-auth portal-escape	Configures portal escape.
Enabling DHCP Address Check	(Optional) It is used to check whether the IP address of a client is allocated by the DHCP server. If not, the client's authentication request is denied.	
	web-auth dhcp-check	Checks whether the IP address of a client is assigned by the DHCP server.
Disabling Link Detection	(Optional) It is used for jitter-off purposes to prevent the deletion of a client's Web authentication entry when the link of the client is disconnected, so that the client can access the Internet again without authentication.	
	no web-auth sta-leave detection	Disables link detection.
Disabling Portal Extension	(Optional) It is used to disable portal extension in order to interwork with CMCC standard portal server. Portal extension must be enabled for interworking with Ruijie portal server software.	
	no web-auth portal extension	Disables portal extension.
Configuring a Whitelist and Blacklist	(Optional) It is used to configure a blacklist to prevent authenticated clients from accessing some network resources, and a whitelist to allow unauthenticated clients to access some network resources.	

Configuration	Description and Command	
	web-auth acl{black-ip *ip*|**black-port** *port*|**black-url** *name*|**white-url** *name***}**	Configures a whitelist and blacklist.
Configuring Jitter-off Accounting	(Optional) It is used to configure whether the jitter-off duration is included into the online duration, in order to improve accounting precision. The jitter-off duration depends on the jitter-off configuration of a specific product.	
	web-auth accounting jitter-off	Configures the jitter-off duration. (Use the **no** form of this command to disable this function.)
	web-auth user-flow-control by-radius-class { **format-16bytes** | **format-32bytes**}	Configures client-based rate limiting.
Configuring the Portal Communication Port	(Optional) It is used to configure the port (source port) used for the communication between the NAS and portal server.	
	ip portal source-interface *interface-type interface-num*	Specifies the port used for the communication between the NAS and portal server.
Configuring a NDKEY-Compatible Webauth URL	(Optional) It is used to configure the Webauth URL used in Web authentication to support the Shanghai NDKEY system.	
	web-auth dkey-compatible url-parameter *string*	Configures a NDKEY-Compatibility compatible between the Shanghai NDKEY system and redirection Webauth URL.
Enabling NAT for Ruijie iPortal Web Authentication	(Optional) It is used to configure Ruijie iPortal Web Authentication to support network address translation (NAT).	
	iportal nat enable	Enables NAT for Ruijie iPortal Web Authentication.
Configuring the iPortal HTTP Retransmission Times	(Optional) It is used to configure the iPortal HTTP retransmission times.	
	iportal retransmit *count*	Configures the iPortal HTTP retransmission times.
Configuring Service Selection in Ruijie iPortal Web Authentication	(Optional) It is used to configure the service type used by Ruijie iPortal Web Authentication.	
	iportal service [**internet** *internet-name* | **local** *local-name*]	Configures the service type used by Ruijie iPortal Web Authentication.
Configuring the Accounting Method List of Web Authentication	(Optional) It is used to configure an accounting method based on the template.	
	web-auth accounting v2 { default | *name***}**	Configures an accounting method based on the template.

Configuration	Description and Command	
Configuring a Web Authentication Method List	(Optional) It is used to configure an authentication method based on the template.	
	web-auth authentication v2 { **default** | *name*}	Configures an authentication method based on the template.
Configuring a Delay for Users to Go Offline Upon Interface Down	**web-auth linkdown-timeout** *timeout*	Configures a delay for the user to go offline upon interface Down.
Configuring RADIUS Authentication Escape	(Optional)	
	web-auth radius-escape	Configures RADIUS authentication escape.
Configuring Noise Reduction in Wireless Web Authentication	**web-auth noise** [**aging** *agmin*] [**hit** *times*]	Configures a noise reduction policy for web authentication.
Enabling iOS Automatic Pop-up Window Control in WeChat-Based Authentication	**http redirect adapter ios**	Enabling iOS Automatic Pop-up Window Control in Global Configuration Mode
Enabling the Smart WeChat Web Authentication	**web-auth sta-perception enable**	Enables MAC Bypass for WeChat authentication.
Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol	(Optional) It is used to configure transparent transmission of the 0x05 attribute of the portal protocol.	
	web-auth portal-attribute [5 | textinfo]	Configures transparent transmission of the 0x05 attribute of the portal protocol.
Configuring Uniqueness Check of Portal Authentication Accounts	(Optional) It is used to configure uniqueness check of portal authentication accounts.	
	web-auth portal-valid unique-name	Configures uniqueness check of portal authentication accounts.
Enabling the One-click Switch Configuration via WiFiDog	(Optional) It is used to enable the one-click switch configuration via WiFiDog.	
	web-auth wifidog-template wlan-range portal-ip nas-ip url [**escape** | **gateway-id** | **perception**]	Enables the one-click switch configuration via WiFiDog.
Enabling the One-click Switch Configuration via WeChat	(Optional) It is used to enable the one-click switch configuration via WeChat.	
	web-auth wechat-template wlan-range portal-ip nas-ip [ios-adapter | perception]	Enables the one-click switch configuration via WeChat.

Configuration	Description and Command	
Enabling the Device to Automatically Add a Domain Name to the Authentication Username	**domain** *domain-string*	Configures the device to automatically add a domain name to the username.

1.4.1. Configuring First-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- (Mandatory)To enable Web authentication successfully, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Setting the SNMP Parameters Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must set the SNMP network management parameters used for the communication between the NAS and portal server.
- The NAS or convergence device and portal server jointly manage authenticated clients through SNMP/MIB. A table of authenticated clients is managed by MIB on the NAS. The portal server is able to access the MIB to obtain client statistics so as to control client login and logout. When a client logs out, the NAS or convergence device will inform the portal server by Webauth Inform packets.

Enabling First-Generation Web Authentication on an Interface

- Mandatory.

- When First-Generation Web Authentication is enabled in WLAN security configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring the First-Generation Webauth Template

Command	**web-auth template eportalv1**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**eportalv1** is the default template of Ruijie First-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** *ip-address*
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** *url-string*
Parameter Description	*url-string*: Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring a URL Format of the Portal Server

Command	**fmt** { **ace** | **default** | **custom** }
Parameter Description	Indicates a URL format of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The **ace** parameter indicates association with ACE.

Specifying the Webauth Binding Mode

Command	**bindmode ip-mac-mode**

Parameter Description	Indicates the Webauth binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Specifying the Redirection Method

Command	**redirect** { **http** | **js** }
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Webauth Communication Key

Command	**web-auth portal key** {*key-string*}
Parameter Description	*key-string:* Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the SNMP-Server Community String

Command	**snmp-server community** {*community-string*}**rw**
Parameter Description	*community-string*: Indicates the community string. **rw**: Must be set to **rw** to support the read and write operations as the Set operation on MIB is required.
Command Mode	Global configuration mode
Usage Guide	The SNMP-server community string is used by the portal server to manage the online clients on the NAS or convergence device.

Configuring the SNMP-Server Host

Command	**snmp-server host** {*ip-address*} **inform version 2c** {*community-string*} **web-auth**
Parameter Description	*ip-address*: Indicates the IP address of the SNMP-server host, that is, the portal server. *community-string*: Configures the community string used to send an SNMP Inform message.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP-server host to receive Webauth messages, including the type, version, community string, and other parameters. **inform:** Enables the SNMP Inform function. The NAS or convergence device will send a message to the portal server when a client logs out. The message type is set to Inform instead of Trap to avoid message loss.

	version 2c: Indicates SNMPv2 for SNMP Inform is not supported in all SNMP versions excluding SNMPv1. **web-auth**: Indicates the preceding parameters to be used for Web authentication. For details regarding SNMP configuration and others, see the *Configuring SNMP*. The SNMP parameter **version 2c**listed here is aimed at SNMPv2. SNMPv3 is recommended if higher security is required for the SNMP communication between the NAS and portal server. To use SNMPv3, change **SNMP Community** to **SNMP User**, **version 2c** to **SNMPv3**, and set SNMPv3-related security parameters. For details, see the *Configuring SNMP*.

Enabling the Webauth Trap/Inform Function

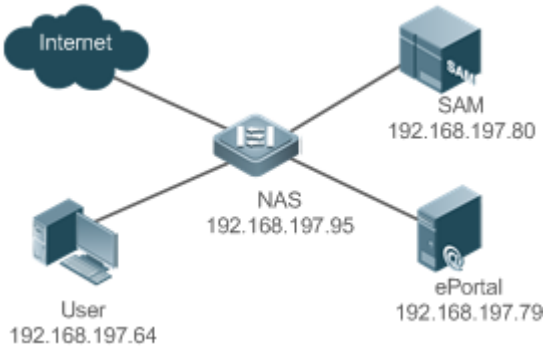
Command	**snmp-server enable traps web-auth**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the NAS or convergence device to send Webauth Trap and Inform messages externally. web-auth: Indicates Web authentication messages.

Enabling First-Generation Web Authentication

Command	**webauth**
Parameter Description	Indicates a Webauth template.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring First-Generation Web Authentication

Scenario Figure 1-7	
Configuratio	● On the NAS, configure the IP address of the ePortal server and the key (webkey) used for

n Steps	communicating with the ePortal server. ● Configure the Webauth URL on the NAS. ● Set the SNMP network management parameters (community string: public) used for the communication between the NAS and ePortal server. ● Enable Web authentication on WLAN 1 on the NAS.
	Hostname# config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#web-auth template eportalv1 Hostname(config.tmplt.eportalv1)#ip 192.168.197.79 Hostname(config.tmplt.eportalv1)#exit Hostname(config)# web-auth portal key webkey
	Hostname(config)# web-auth template eportalv1 Hostname(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp Hostname(config.tmplt.eportalv1)#exit
	Hostname(config)# snmp-server community public rw Hostname(config)# snmp-server enable traps web-auth Hostname(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth Hostname(config)# exit
	Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal eportalv1 Hostname(config-wlansec)# webauth
Verification	● Check whether Web authentication is configured successfully.
	Hostname(config)#show running-config ... snmp-server host 192.168.197.79 inform version 2c public web-auth snmp-server enable traps web-auth snmp-server community public rw ... web-auth template eportalv1 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp ! web-auth portal key webkey

	... wlansec 1 web-auth portal eportalv1 webauth
	Hostname#show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- wlansec 1 On eportalv1 0
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv1 BindMode: ip-mac-mode Type: v1 Ip: 192.168.197.79 Url: http://192.168.197.79:8080/eportal/index.jsp

Common Errors

- The SNMP parameters used for the communication between the portal server and NAS are configured incorrectly, causing authentication failures.
- Specify the IP-MAC binding mode to deploy Web authentication on layer-3 networks, causing authentication failures.
- When Web authentication is used in conjunction with VRRP, run the snmp-server trap-source ip command to specify the VRRP address; otherwise, the portal server cannot process Trap packets correctly.

1.4.2. Configuring Second-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. IPv6 is supported.

Notes

- Second-Generation Web Authentication complies with the CMCC WLAN Service Portal Specification. Furthermore, it is extended to support Ruijie portal server. Perform compatible configuration based on the server performance in actual deployment. For details, see the subsequent chapter.
- When you configure the URL of the second-generation portal server, if the URL contains an IPv6 address, enclose it with a pair of square brackets, for example, http://[2001::1]/index.jsp.

- The cmcc-normal and cmcc-ext1 parameters in the fmt command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid.

Configuration Steps

Enabling AAA

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Ruijie Second-Generation Web Authentication.

Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Configuring an AAA Method List for Web Authentication

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure an AAA authentication method list.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

Configuring an AAA Method List for Web Accounting

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure an AAA method list for Web accounting.
- An accounting method list is used to associate an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the Portal Server

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Configuring the Portal Server in Global or Interface Configuration Mode

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must specify the use of the second generation portal server in global or interface configuration mode.
- The NAS first selects the portal server in interface configuration mode. If such a portal server does not exist, the NAS selects the portal server in global configuration mode. If such a portal server does not exist, eportalv1 is used by default. The NAS redirects users to the selected portal server.

Enabling Ruijie Second-Generation Web Authentication on an Interface

- Mandatory.
- When Ruijie Second-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** {*ip-address*} [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** {*string*}
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command	Global configuration mode

Mode	
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS authentication method.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS accounting method.

Configuring the Second-Generation Webauth Template

Command	**web-auth template**{**eportalv2 |** *portal-name* **v2**}
Parameter Description	*portal-name*: Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of Ruijie Second-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* | *ipv6-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** *url-string*
Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt** {**cmcc-ext1 | cmcc-ext2 cmcc-normal | default | cmcc-mtx | cmcc-ext3 | ct-jc | cucc | custom**}
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode

Usage Guide	The **cmcc-normal** and **cmcc-ext1** parameters in the **fmt** command support only IPv4. The **default** parameter indicates the default format. The **custom** parameter indicates the custom format. The **cmcc-ext2** is supported for Liaoning CMCC. When **fmt** is set to **cmcc-mtx**, the URL format of mobile AC vendors is supported. The **ct-jc** format is supported for Chine Telecom. The **cucc** format is supported for Shandong China Telecom. The **custom** format is defined by users.

Configuring a User Binding Mode

Command	**bindmode ip-mac-mode**
Parameter Description	Indicates a user binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Specifying the Encapsulation Format of the Webauth URL

Command	**redirect { http | js }**
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Webauth Communication Key

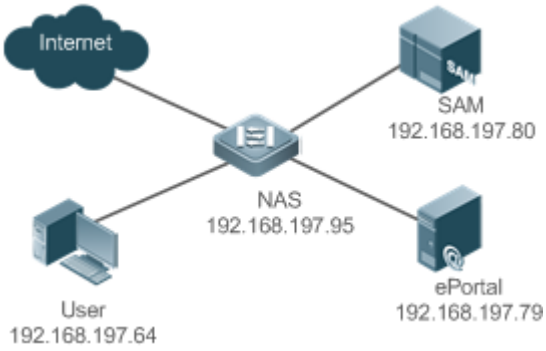
Command	**web-auth portal key** *key-string*
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Second-Generation Web Authentication

Command	**webauth**
Parameter Description	Indicates a Webauth template.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring Ruijie Second-Generation Web Authentication

Scenario Figure 1-8	
Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS-server host and communication key on the NAS. ● Configure the default AAA method lists for Web authentication and accounting on the NAS. ● Configure the IP address of the portal server and the Webauth communication key (webkey) used for communicating with the portal server on the NAS. ● Configure the Webauth URL on the NAS. ● Configure Ruijie Second-Generation Web Authentication in global configuration mode on the NAS. ● Enable Web authentication on WLAN 1 of the NAS.
	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#aaa new-model
	Hostname(config)#radius-server host 192.168.197.79 key webkey
	Hostname(config)#aaa authentication web-auth default group radius Hostname(config)#aaa accounting network default start-stop group radius
	Hostname(config)#web-auth template eportalv2 Hostname(config.tmplt.eportalv2)#ip 192.168.197.79 Hostname(config.tmplt.eportalv2)#exit Hostname(config)#web-auth portal key ruijie
	Hostname(config)# web-auth template eportalv2 Hostname(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp Hostname(config.tmplt.eportalv2)#exit
	Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal eportalv2 Hostname(config-wlansec)# webauth Hostname(config-wlansec)# exit

Verification	● Check whether Web authentication is configured successfully.
	Hostname(config)#show running-config ... aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius ... radius-server host 192.168.197.79 key webkey ... web-auth template eportalv2 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp ! web-auth portal key ruijie ... wlansec 1 web-auth portal eportalv2 webauth !
	Hostname#show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- wlansec 1 On eportalv2 0
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 BindMode: ip-mac-mode Type: v2 Port: 50100 Ip: 192.168.197.79 Url: http://192.168.197.79:8080/eportal/index.jsp Wechat enable: 0

	Temporary permit:0

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the *CMCC WLAN Service Portal Specification*, causing compatibility failure.

1.4.3. Configuring iPortal Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. No external portal server is required.

Notes

- Some devices, such asAP110, do not have a built-in page suite. You need to import a page suite before use. For details about the page suite support on a product, see the corresponding product description.
- Ruijie iPortal Web Authentication is configured on EG devices in global configuration mode.
- To configure a customized page suite, the configuration must comply with the relevant specification.

Configuration Steps

↘ Enabling AAA

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must enable AAA.
- The iPortal NAS is responsible for initiating authentication to the portal server through AAA in Ruijie iPortal Web authentication.

↘ Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable Ruijie iPortal Web Authentication, you must configure the RADIUS-server host.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

↘ Configuring an AAA Method List for iPortal Web Authentication

- (Mandatory) To enable iPortal Web Authentication, you must configure an AAA method list for Ruijie iPortal Web Authentication.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

↘ Configuring an AAA Method List for iPortal Web Accounting

- (Optional) Some servers require that authentication and accounting be enabled. Configure Web accounting based on the characteristics of the server in use.
- An AAA accounting method list associates an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the iPortal Webauth Template

- Mandatory.
- If any non-default authentication and accounting method lists are configured, you need to specify the name of a method list in template configuration mode; otherwise, the default method list is used.

Enabling iPortal Web Authentication

- Mandatory.
- If web authentication is enabled on a WLAN network, all users accessing the WLAN network need to perform web authentication.

Verification

- Check whether unauthenticated clients are redirected to the Webauth URL to perform authentication, and the Webauth URL displayed is that in the page suite.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** { *ip-address* } [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS-server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Ruijie iPortal Web Authentication

Command	**aaa authentication iportal** { **default** | *list-name* } *method1* [*method2*...]

Parameter Description	*list-name*: Creates a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	The specified AAA method should exist in the AAA configuration.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	The specified AAA method should exist in the AAA configuration.

Configuring the iPortal Webauth Template

Command	**web-auth template iportal**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Pre-login Advertisement Mode

Command	**login-popup** *url-string*
Parameter Description	Indicates the advertisement URL.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Specifying the Post-login Advertisement Mode

Command	**online-popup** url-string
Parameter Description	Indicates the advertisement URL.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Customizing a Page Suite

Command	**page-suit** *filename*
Parameter Description	Indicates the file name of a page suite.

Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the iPortal Advertisement Interval

Command	**time-interval** *hour*
Parameter Description	Indicates the advertisement interval.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Enabling iPortal Web Authentication

Command	**webauth**
Parameter Description	Indicates the customized template name.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring Ruijie iPortal Web Authentication

Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS-server host and communication key on the NAS. ● Configure the default AAA authentication and accounting method lists on the NAS. ● Configure the global use of the iPortal server on the NAS. ● Enable Web authentication on wlan 1 on the NAS.
	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# aaa new-model
	Hostname(config)# radius-server host 192.168.197.79 key webkey
	Hostname(config)# aaa authentication iportal default group radius Hostname(config)# aaa accounting network default start-stop group radius
	Hostname(config)#web-auth template iportal
	Hostname(config.tmplt.iportal)# accounting default Hostname(config.tmplt.iportal)# authentication default Hostname(config.tmplt.iportal)# page-suite defaul Hostname(config.tmplt.iportal)# exit

	Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal iportal Hostname(config-wlansec)# webauth
Verification	● Check whether Ruijie iPortal Web Authentication is configured successfully.
	Hostname(config)#show running-config ... aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius ... radius-server host 192.168.197.79 key webkey ... web-auth template iportal page-suite default authentication default accounting default ! ... wlansec 1 web-auth portal iportal webauth
	Hostname# show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- wlansec 1 On iportal 0
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: iportal BindMode: ip-mac-mode Type: intra Port: 8081

	time_interval: 1 Login_popup: (null) Online_popup: (null) Suitename: default Authentication: default Accounting: default ...

Common Errors

- The preparation of a page suite does not comply with the relevant specification.
- A page suite is specified, but is not downloaded to the flash memory or the specified directory.

1.4.4. Configuring WiFiDog Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- (Mandatory) To enable Web authentication, you must configure and apply the portal server.
- When the NAS finds an unauthenticated client attempting to access network resources through HTTP, it redirects the client's access requests to the specified Webauth URL, where the client can initiate authentication to the portal server. The IP address of the portal server is configured as a network resource which clients can access without authentication. Unauthenticated clients can directly access this IP address through HTTP.

Configuring the IP Address of the NAS

- Mandatory.
- By default, the IP address of the NAS is not configured.
- Ensure that the configured IP address is accessible by clients.

Enabling WiFiDog Authentication in WLAN Security Configuration Mode

- Mandatory.
- Web authentication is not enabled by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring a WiFiDog Webauth Template

Command	**web-auth template** { **wifidog** | *template-name* **wifidog** }
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**wifidog** means the default WiFiDog Webauth template.

Configuring the IP Address of the Portal Server

Command	**ip** *ip-address*
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Web authentication template configuration mode
Usage Guide	N/A

Configuring the Gateway ID

Command	**gateway-id** *string*
Parameter Description	*string*: Indicates the gateway ID used in WiFiDog.
Defaults	It is the serial number of the device by default.
Command Mode	Web authentication template configuration mode
Usage Guide	This parameter is carried in the WiFiDog packets and provided for the interconnected third-party portal. This parameter is optional in the stand-along mode.

Configuring the Webauth URL of the Portal Server

Command	**url** *url-string*
Parameter Description	*url-string*:Indicates the Webauth URL of the portal server.The maximum length of this address is 255 bytes.
Command Mode	Web authentication template configuration mode
Usage Guide	The URL starts with **http://** or **https:**//.

Configuring the IP Address of the NAS

Command	**nas-ip** { *ip-address* }

Parameter Description	Indicates the IP address of the NAS.
Command Mode	Web authentication template configuration mode
Usage Guide	Ensure that the configured IP address is accessible by clients.

Configuring the Portal Server in Global or WLAN Security Configuration Mode

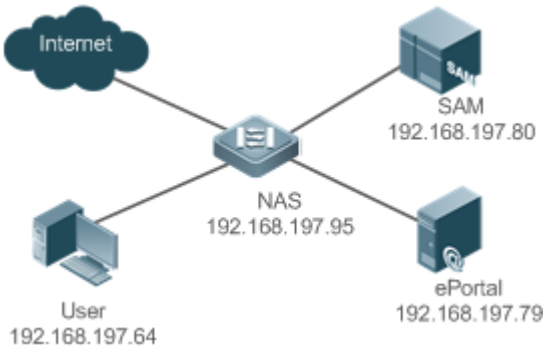
Command	**web-auth portal** { *template-name* | **wifidog** }
Parameter Description	*template-name*: The name of the customized WiFiDog authentication template. **wifidog**: The name of the default WiFiDog authentication template.
Defaults	*N/A*
Command Mode	WLAN security configuration mode Global configuration mode
Usage Guide	N/A

Enabling WiFiDog Web Authentication on an Interface

Command	**webauth**
Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring WiFiDog Web Authentication

Scenario Figure 1-9	
Configuration Steps	● Configure the IP address of the portal server on the NAS. ● Configure the Webauth URL on the NAS. ● Configure the IP address used for external communication on the NAS. ● Enable WiFiDog Web authentication for WLAN10 on the NAS.

	Hostname# config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#web-auth template wifidog Hostname(config.tmplt.wifidog)# ip 192.168.197.79
	Hostname(config.tmplt.wifidog)# url http://192.168.197.79/auth/wifidogAuth Hostname(config.tmplt.wifidog)# nas-ip 192.168.197.95 Hostname(config.tmplt.wifidog)# exit
	Hostname(config)# wlansec 10
	Hostname(config-wlansec)# web-auth portal wifidog Hostname(config-wlansec)# webauth Hostname(config-wlansec)# exit
Verification	● Check whether WiFiDog Web authentication is configured successfully.
	Hostname(config)#show running-config ... web-auth template wifidog ip 192.168.197.79 nas-ip 192.168.197.95 url http://192.168.197.79/auth/wifidogAuth ... wlansec 10 web-auth portal wifidog webauth
	Hostname#show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- wlansec 10 On wifidog 0 ...
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: wifidog Type: wifidog Ip: 192.168.197.79

	Url: http://192.168.197.79/auth/wifidogAuth NasIp: 192.168.197.95 .....

Common Errors

- The IP address of the NAS is not configured, causing a redirection failure.

1.4.5. Configuring MAC Address-Based SMS Authentication

Configuration Effect

Allow unauthenticated clients connected to WLAN to access network resources. When a user uses up the traffic during the specified time period, the NAS initiates a MAC address binding query to the bound portal server. If the user is bound with a MAC address, the portal server initiates an authentication request. If the STA is not bound with a MAC address, the STA needs to perform authentication on the portal server before accessing the Internet.

Notes

- MAC address-based SMS authentication is supported only on wireless devices.
- The configured URL of the portal server must adopt the **cmcc-ext1** format.

Configuration Steps

↘ Enabling AAA

- (Mandatory) To enable MAC address-based SMS authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Ruijie Second-Generation Web Authentication.

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

↘ Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable MAC address-based SMS authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Command	**radius-server host** { *ip-address* } [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** { *string* }

Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure an AAA authentication method list on the AAA module.
- A Web authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the Web authentication method list.

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Indicates a method list name. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS authentication method.

Configuring an AAA Method List for Web Accounting

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure a network accounting method on the AAA module.
- A network accounting method is used to associate an accounting method and server. In Web authentication, accounting is implemented to record user information or fees.

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Indicates a method list name. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	Second-Generation Web Authentication adopts the RADIUS accounting method.

Configuring the Second-Generation Webauth Template

- (Mandatory) To enable Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Command	**web-auth template** { **eportalv2 |** *portal-name* **v2**}

Parameter Description	Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of Ruijie Second-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* | *ipv6-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** *url-string*
Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt { cmcc-ext1 | cmcc-normal | default }**
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	**fmt** must be set to **cmcc-ext1**.

Configuring the Webauth Communication Key

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Command	**web-auth portal key** *key-string*
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Detection Interval and Traffic Threshold for MAC Address-based SMS Authentication

- After an STA is associated with the WLAN enabled with MAC address-based SMS authentication, a free data quota is allocated to the STA. When the STA uses up the traffic allowed during the specified time period, a MAC address binding status query is triggered.

Command	**web-auth sms-flow interval** *interval* **threshold** *flows*
Parameter Description	*interval*: Indicates the detection interval, in the unit of minutes. *flows*: Indicates the flow threshold, in the unit of KB.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Portal Server Bound for MAC Address-based SMS Authentication

- Mandatory.

Command	**web-auth bind-portal** *string* **[type {** *local-spec* **|** *group-spec***}]**
Parameter Description	*string*: Indicates a Webauth template.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Setting the winterface Field in the Redirection URL

- China Mobile's MAC address-based specification requires that the redirection URL carry the **winterface** field, which must be configurable based on a WLAN.

Command	**web-auth winterface** *string*
Parameter Description	*string*: Indicates **winterface** field.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Setting the AC IP Field in the Redirection URL

- China Mobile's MAC address-based specification requires that the redirection URL carry the **AC IP** field. Because an AC may have multiple IP addresses, a configuration command is provided to configure an IPv4 address on the specified WLAN, and the IPv4 address specifies the value of the **AC IP** field in the redirection URL.

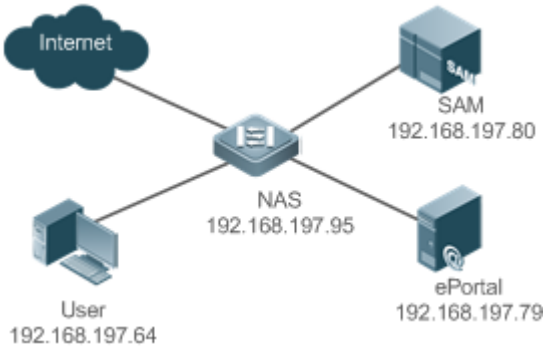
Command	**web-auth wlan-ac-ip** *ipv4*
Parameter Description	*ipv4:* Indicates the **AC IP** field.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

- Check that unauthenticated clients can access the Internet before the traffic threshold is reached.
- Check that authentication is triggered when the traffic threshold is reached.

Configuration Example

↘ Configuring MAC Address-Based SMS Authentication

Scenario Figure 1-10	
Configuration Steps	• Enable AAA on the NAS. • Configure the RADIUS-server host and communication key on the NAS. • Configure the default AAA method lists for Web authentication and accounting on the NAS. • Configure the IP address of the portal server and the Webauth communication key (webkey) used for communicating with the portal server on the NAS. • Configure the Webauth URL on the NAS. • Configure the detection interval and traffic threshold for MAC address-based SMS authentication, and set the **winterface** and **AC IP** fields on the NAS. • Enable MAC address-based SMS authentication for WLAN 1 on the NAS.
	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#aaa new-model
	Hostname(config)#radius-server host 192.168.197.79 key webkey
	Hostname(config)#aaa authentication web-auth default group radius Hostname(config)#aaa accounting network default start-stop group radius
	Hostname(config)#web-auth template eportalv2 Hostname(config.tmplt.eportalv2)#ip 192.168.197.79 Hostname(config.tmplt.eportalv2)#exit Hostname(config)#web-auth portal key webkey
	Hostname(config)# web-auth template eportalv2 Hostname(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp

	Hostname(config.tmplt.eportalv2)#fmt cmcc-ext1 Hostname(config.tmplt.eportalv2)#exit
	Hostname(config)# web-auth sms-flow interval 5 threshold 10 Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth bind-portal eportalv2 type group-spec Hostname(config-wlansec)# web-auth accounting v2 default Hostname(config-wlansec)# web-auth authentication v2 default Hostname(config-wlansec)# webauth Hostname(config-wlansec)# exit
Verification	● Check whether Web authentication is configured successfully.
	Hostname(config)#show running-config ... aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius ... radius-server host 192.168.197.79 key webkey ... web-auth template eportalv2 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp fmt cmcc-ext1 ! web-auth portal key webkey web-auth sms-flow interval 5 threshold 10 ... ! wlansec 1 web-auth bind-portal eportalv2 type group-spec web-auth accounting v2 default web-auth authentication v2 default webauth

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the CMCC WLAN Service Portal Specification, causing compatibility failure.

1.4.6. Configuring WeChat Web Authentication

Configuration Effect

- Redirect unauthenticated mobile phone users with WLAN association to a WeChat-based one-click Wi-Fi connection page displayed on the mobile phone browser. A user can tap a link on the page to wake up the WeChat client and use it to perform Wi-Fi connection authentication.
- Allow unauthenticated mobile phone users to scan a QR code to perform Wi-Fi connection authentication through WeChat.
- Redirect unauthenticated PC users with WLAN association to a WeChat-based one-click Wi-Fi connection page displayed on the PC browser. A user can scan a QR code on the page by using the mobile phone associated with the same WLAN as the PC to enable the PC to perform authentication to access the Internet.

Notes

- WeChat Web authentication is supported only on wireless devices.

Configuration Steps

↘ Creating a Wechat Webauth Template

- (Mandatory) To enable WeChat Web authentication, you must create a template.

Command	**web-auth template** { **wechat** | *portal-name* **wechat** }
Parameter Description	Indicates the name of the customized template for WeChat Web authentication
Command Mode	Global configuration mode
Usage Guide	**wechat** is the name of the default template of WeChat-based Wi-Fi connection authentication.

↘ Configuring the IP Address of the Portal Server

- (Mandatory) To enable WeChat Web authentication, you must configure the IP address of the portal server.

Command	**ip** *ip-address*
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode

Usage Guide	N/A

Configuring the WeChat Webauth URL

- (Mandatory) To enable WeChat Web authentication, you must configure the WeChat Webauth URL address of the portal server.

Command	**service-url** { *url-string* }
Parameter Description	Indicates the WeChat Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	Configure only the domain name, which must not start with **http://** or **https://**.

Configuring the Authentication Page Address for the Portal Server

- The function is optional for devices of version 11.1(5)B9 and the default configuration can be used.

Command	**url** { *url-string* }
Parameter Description	**url**: Indicates the URL address of the server.
Command Mode	Template configuration mode of web authentication
Usage Guide	The authentication page address starts with **http://** or **https://**.

Configuring the Webauth Communication Key

- (Mandatory) To enable WeChat Web authentication, you must configure the communication key of the portal server.

Command	**key** *key-string*
Parameter Description	*key-string*: Indicates the communication key of the portal server. You need to configure a key used for the communication between the NAS and authentication server. The key contains up to 255 characters.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the communication keys configured on the portal server and the NAS are the same; otherwise, interworking will fail.

Enabling the Smart WeChat Web Authentication

- Optional.

Command	**web-auth sta-perception enable**
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Enable the smart authentication based on customer's requirements. Run the **ip dhcp snooping** command before the smart authentication takes effect.

Enabling the Collective Escape Function

- (Optional) After the function is enabled, the device starts counting single escape users. If the number of single escape users reaches the threshold within a certain interval, the device starts collective escape and all users who gain access later are permitted to pass without authentication.
- In WLANSEC configuration mode, this function is supported in the version 11.1(5)B23. Configuration in WLANSEC configuration mode takes precedence. If this feature is not configured in WLANSEC configuration mode, then configuration in global configuration mode takes effect.
- To cancel collective escape, run the **web-auth wechat-escape recover** command in global configuration mode to restore the single escape state.

Command	**web-auth wechat-escape interval** *minutes* **times** *count*
Parameter Description	*minutes*: Indicates timer interval for judging collective escape. The unit is minutes and the default value is 60 minutes. *count*: Indicates the user quantity threshold. The default value is 5.
Command Mode	Global configuration mode
Usage Guide	In WLANSEC configuration mode, this function is supported in the version 11.1(5)B23.

Configuring Server Detection

- (Optional) After the function is configured, the device detects the server. If it fails to receive the server response or the response is unavailable within a certain interval and the collective escape function is configured on the device, all users who gain access later are permitted to pass without authentication.
- To cancel server detection, run the **no web-auth wechat-check** command in global configuration mode.

Command	**web-auth wechat-check interval** *minutest*
Parameter Description	*minutes*: Indicates the timer interval for server detection. The unit is minutes and there is no default value.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Temporary Permit Function

- (Optional) The temporary permit function permits the packets sent by STAs to pass through during the authentication process. (The packets exchanged with the MCP server and Tencent server are permitted to pass through, whereas blacklist requests, login authorization requests, forced follow-up requests, and other requests are intercepted for processing.)

Command	**temporary-permit** *seconds*
Parameter Description	*seconds*: Indicates the duration of temporary permit in the unit of seconds. The recommended value ranges from 1s to 65535s.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Smart IP Address Check

- (Optional) After smart IP address check is configured, the STAs that fail to obtain IP addresses after the specified time has elapsed are forced offline.

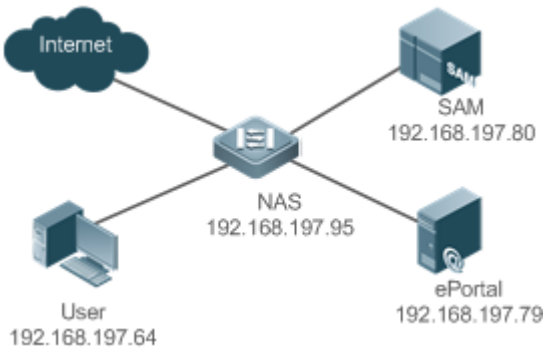
Command	**web-auth valid-ip-acct[timeout** *seconds***]**
Parameter Description	*seconds*: Indicates the time during which STAs can attempt to obtain IP addresses in the unit of seconds. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Configuration Example

Configuring WeChat Web Authentication

Scenario Figure 1-11	
Configuration Steps	• Configure the IP address 192.168.58.110 of the domain name server on the NAS. • Configure the WeChat Webauth template on the NAS. • Configure the IP address and Webauth URL on the NAS. • Configure the communication key (ruijie) used for communicating with the portal server on the NAS. • Configure the IP address used for external communication on the NAS. • Configure the WeChat Webauth version as 1.0 on the NAS. • Apply the template to WLANSEC1 and enable WeChat Web authentication.
	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#ip name-server 192.168.58.110
	Hostname(config)#web-auth template wechat
	Hostname(config.tmplt.wechat)#ip 192.168.197.79

	Hostname(config.tmplt.wechat)#service-url wmc.ruijie.com.cn
	Hostname(config.tmplt.wechat)#key ruijie
	Hostname(config.tmplt.wechat)#nas-ip 192.168.197.104
	Hostname(config.tmplt.wechat)#version 1.0 Hostname(config.tmplt.wechat)#exit
	Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal wechat Hostname(config-wlansec)# webauth
Verification	Check whether Web authentication is configured successfully.
	Hostname(config)#show running-config ... ip name-server 192.168.58.110 ... web-auth template wechat ip 192.168.197.79 service-url wmc.ruijie.com.cn http://192.168.197.79:8080/eportal/index.jsp key ruijie nas-ip 192.168.197.104 !... wlansec 1 web-auth portal wechat webauth !

Common Errors

- The key used for the communication between the portal server and NAS is configured incorrectly, or encryption is configured only on the portal server or NAS, causing abnormal authentication.
- The IP address of the NAS is configured as a authentication-free address, and authentication packets cannot be received, causing an authentication failure.
- The IP address of the domain name server is not configured, causing a whitelist resolution failure. The IP address of the WeChat server is not permitted to pass.

- The ip dhcp snooping, ip dhcp snooping trust, and web-auth sta-perception enable commands are not executed when smart authentication is enabled, causing a failure of the smart authentication during second-time authentication.

1.4.7. Specifying an Authentication Method List

Configuration Effect

- The portal server sends an authentication request to the NAS when a user submits authentication information. The NAS resolves the authentication server information and other information based on the configured authentication method list name before initiating authentication.
- The NAS selects the authentication server based on the specified authentication method list.

Notes

- Before you configure an authentication method list name, ensure that the authentication methods in the list have been configured on the AAA module. The command used to configure authentication methods on the AAA module is **aaa authentication web-auth** { *default* | *list-name* }*method1 [method2*...].
- Different authentication methods for IPv4 authentication and IPv6 authentication are not supported.

Configuration Steps

- Optional.
- The default authentication method is used if no authentication method list is configured. Run the **authentication** { *mlist-name* } command to configure an authentication method list name when the authentication method list name on the AAA module needs to be modified or multiple method lists exist.

Verification

- Configure two authentication method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Create user a and configured a password for the user on server 1. Create user b on server 2.
- Configure the use of list 1.
- Perform authentication as user b and check that authentication fails.
- Perform authentication as user a and check that authentication is successful.

Related Commands

↘ Specifying an Authentication Method List

Command	**authentication** {*mlist-name*}
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured authentication method list name is consistent with that on the AAA

	module.

Configuration Example

↘ Specifying an Authentication Method List

Configuration Steps	● Specify the authentication method list **mlist1**.
	Hostname(config.tmplt.iportal)#authentication mlist1
Verification	● Check whether the configuration is successful.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 50100 State: Active Acctmlist: default Authmlist: mlist1

1.4.8. Specifying an Accounting Method List

Configuration Effect

- The NAS sends an accounting request when a user passes authentication. The recipient of the request depends on the configuration of the accounting method list and is usually the portal server.
- Specify an accounting method list for the NAS to perform accounting.

Notes

- Ensure that the accounting method list has been configured on the AAA module. The command used to configure accounting methods on the AAA module is **aaa accounting network** {**default** | *list-name* }start-stop method1 [method2...].
- Different accounting methods for IPv4 authentication and IPv6 authentication are not supported.

Configuration Steps

- Optional.
- The default accounting method is used if no accounting method list is configured. Run the **accounting** {*mlist-name* } command to configure an accounting method list name when the accounting method list name on the AAA module needs to be modified or multiple method list names exist.

Verification

- Configure two accounting method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Configure the use of list 1.
- Use a valid account to perform authentication to access the Internet.
- View user accounting information on server1 and server2. Check that the user accounting information exists only on server1.

Related Commands

↘ Specifying an Accounting Method List

Command	**accounting**{*mlist-name*}
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured accounting method list name is consistent with that on the AAA module.

Configuration Example

↘ Specifying an Accounting Method List

Configuration Steps	● Specify the accounting method list **mlist1**.
	Hostname(config.tmplt.eportalv2)#accounting mlist1
Verification	● Check whether the configuration is successful.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 50100

Configuration Steps	● Specify the accounting method list **mlist1**.
	Hostname(config.tmplt.eportalv2)#accounting mlist1
Verification	● Check whether the configuration is successful.
	State: Active Acctmlist: mlist1 Authmlist: mlist1

1.4.9. Configuring the Communication Port of the Portal Server

Configuration Effect

- When the NAS detects that a user logs out, it notifies the portal server. The NAS interacts with the portal server through the portal specification, which specifies the port number used to listen to and send/receive packets.
- When the listening port of the portal server is changed, the communication port of the portal server must be modified on the NAS to enable the NAS to interact with the portal server.
- In Ruijie iPortal Web Authentication, this function is used to configure the HTTP listening port of the NAS. The default port number is 8081.

Notes

- The configured port number must be consistent with the port actually used by the portal server.
- This function is applicable to Ruijie Second-Generation Web Authentication and iPortal Web Authentication. The two authentication schemes use different default port numbers. In Ruijie Second-Generation Web Authentication, the configured port number is used for the interaction between the NAS and portal server through the portal specification. In Ruijie iPortal Web Authentication, the configured port number is used for packet listening on the NAS.

Configuration Steps

- Optional.
- Run the **port** *port-num* command to maintain port configuration consistency when the portal server does not use the default port number or the listening port of the NAS conflicts with other port and needs to be adjusted.

Verification

- Configure Ruijie Second-Generation Web Authentication.
- Change the listening port of the server to 10000.
- Run the **port** *port-num* command to configure the port number 10000.

- Simulate the scenario where a user performs authentication to access the Internet.
- Force the user offline on the NAS, refresh the online page, and check that a user logout notification is displayed.

Related Commands

Configuring the Communication Port of the Portal Server

Command	**port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Communication Port of the Portal Server

Configuration Steps	● Configure the communication port of the portal server as port 10000.
	Hostname(config.tmplt.eportalv2)#port 10000
Verification	● Check whether the configuration is successful.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 10000 Acctmlist: Authmlist:

1.4.10. Specifying the Webauth Binding Mode

Configuration Effect

- When a user goes online, the user's entry needs to be written to a forwarding rule. The forwarding rule mapping method can be modified by specifying different binding modes, which further affects the Internet access rules applied to users. In IP-only mode, all the packets carrying the specified IP address are permitted to pass, and the STAs who send the packets can access the Internet. In IP+MAC mode, only the packets carrying both the specified IP address and MAC address are permitted to pass, and the STAs who send the packets can access the Internet.

Notes

- In Layer-3 authentication, the MAC addresses visible to the NAS are the gateway addresses of STAs. Because these MAC addresses are not accurate, the IP-only mode should be used.

Configuration Steps

- (Optional) The default Webauth binding mode is IP+MAC.
- Determine a binding mode based on the accuracy of user information obtained by the NAS. When the IP and MAC addresses of STAs are accurate (in L2 authentication, for example), IP+MAC is recommended. When the IP and MAC addresses are not accurate, select IP-only.

Verification

- Change the binding mode to IP-only.
- Simulate the scenario where a user performs authentication to access the Internet.
- Modify the MAC address of the user, or use a client with the same IP address but a different MAC address to access the Internet.
- Check that the user accesses the Internet normally.

Related Commands

Specifying the Webauth Binding Mode

Command	**bindmode ip-mac-mode**
Parameter Description	**ip-mac-mode**: Indicates IP-MAC binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Specifying the Webauth Binding Mode

Configuration Steps	• Set the binding mode to IP-mac-mode.
	Hostname(config.tmplt.eportalv2)# bindmode ip-mac-mode
Verification	• Check whether the configuration is successful.

Configuration Steps	● Set the binding mode to IP-mac-mode.
	Hostname(config.tmplt.eportalv2)# bindmode ip-mac-mode
Verification	● Check whether the configuration is successful.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 10000 Acctmlist: Authmlist:

1.4.11. Customizing a Page Suite

Configuration Effect

- Configure a page suite to be used on the iPortal server and add special content or information to the page suite, for example, a logo or notice.

Notes

- A page suite must be downloaded manually to the flash memory of the NAS and saved to the ./portal directory. If the page suite is not saved or is saved to an incorrect directory, page push will fail, causing Web authentication invalid. The default page suite can be used if there are no special requirements.

Configuration Steps

- (Optional) By default, the default page suite is used.

Verification

- Configure Ruijie iPortal Web Authentication.
- Download a page suite.
- Specify the page suite.
- Check whether the page suite is applied to the login page.

Related Commands

Customizing a Page Suite

Command	**page-suite** *filename*
Parameter Description	*filename*: Indicates the file name of a page suite.
Command Mode	Webauth template configuration mode
Usage Guide	Download the page suite to be used to the **./porta/zipl** directory of the flash memory in advance.

Configuration Example

Customizing a Page Suite

Configuration Steps	● Customize a page suite.
	Hostname(config.tmplt.iportal)#page-suite hostpage
Verification	● Check whether the configuration is successful.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: iportal Page-suit: hostpage Advertising url: default Advertising mode: online-popup Type: Intral Portal Acctmlist:default Authmlist:default

1.4.12. Configuring the Advertisement Pushing Mode

Configuration Effect

- Optional. Advertisements are pushed before or after authentication.

Notes

- By default, advertisements are pushed after authentication is successful.
- To ensure that only advertisements are pushed in the case that users are not authenticated, select the advertising function. For details, see the advertising configuration manual.

Configuration Steps

- (Optional) By default, advertisements are pushed after the authentication is successful.

Verification

- Configure embedded portal Web authentication.
- Configure a URL address that can access the Internet.
- When a user accesses the network, check whether a new window is displayed after the authentication is successful and whether information on a page of a specific URI is displayed.

Related Commands

Configuring the Advertisement Pushing Address

Command	**login-popup** *url*
Parameter Description	*url*: Indicates the URL popping up before the authentication or upon login.
Command Mode	Web authentication template configuration mode
Usage Guide	N/A

Command	**online-popup** *url*
Parameter Description	*url*: Indicates the URL popping up after successful authentication.
Command Mode	Web authentication template configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Advertisement Pushing Mode

Configuration Steps	• Configure the advertisement pushing mode to advertisement pushing before authentication.
	Hostname(config.tmplt.iportal)#login-popup http://www.host.com Hostname(config.tmplt.iportal)#popup mode login-popup
Verification	• Check whether the advertisement pushing mode is configured successfully.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: iportal BindMode: ip-mac-mode Type: intra Port: 8081

Configuration Steps	● Configure the advertisement pushing mode to advertisement pushing before authentication.
	Hostname(config.tmplt.iportal)#login-popup http://www.host.com Hostname(config.tmplt.iportal)#popup mode login-popup
Verification	● Check whether the advertisement pushing mode is configured successfully.
	time_interval: 1 Login_popup: http://www.host.com Online_popup: (null) Suitename: default Authentication: Accounting:

1.4.13. Configuring a Custom URL Format

Configuration Effect

- The redirection URL follows the configured custom format.

Notes

- The parameters in the custom format may not be in the same order as that of the actual URL.

Configuration Steps

- Optional.

Verification

- Configure a custom URL.
- An unauthorized PC accesses the Internet through the port using a browser.
- The access request is redirected. The redirection URL follows the same format as the custom URL.

Related Commands

↘ Configuring a Custom URL Format

Command	**fmt custom [encrypt { md5 | des | des_ecb | des_ecb3 | none }] [user-ip** *userip-str* **] [user-mac** *usermac-str* **mac-format [dot | line | none | 5colon]] [user-vid** *uservid-str* **]** [**user-id** *userid-str*] **[nas-ip** *nasip-str* **] [nas-id** *nasid-str* **] [nas-id2** *nasid2-str* **] [ac-name** *acname-str* **] [ap-mac** *apmac-str* **mac-format [dot | line | none]] [url** *url-str* **] [ssid** *ssid-str* **] [port** *port-str* **] [ac-serialno** *ac-sno-str* **] [ap-serialno** *ap-sno-str* **] [additional** *extern-str* **]**
Parameter Description	*userip-str*: Indicates the name of the user IP address parameter. *usermac-st*: Indicates the name of the user MAC address parameter. *uservid-str*: Indicates the name of the user VID parameter.

	userid-str: Indicates the name of the user ID parameter. *nasip-st*: Indicates the name of the NAS IP address parameter. *nasid-str*: Indicates the name of the NAS ID parameter. *nasid2-str*: Indicates the name of an NAS ID parameter (two NAS ID parameters are supported). *ac-name*: Indicates the name of the NAS name parameter. *apmac-str*: Indicates the name of the AP MAC address parameter. *apmac-str*: Indicates the name of the original URL parameter. *ssid-str*: Indicates the name of the SSID parameter. *port-str*: Indicates the name of the authentication port parameter. *ac-sno-st*: Indicates the name of the AC serial number parameter. *ap-sno-st*: Indicates the name of the AP serial number parameter. *extern-st*: Indicates the fixed string, which is required by some Portal servers. *md5*: Indicates MD5 encryption. *des*: Indicates DES encryption. *des_ecb*: Indicates that all parameters adopt des_ecb encryption. *des_ecb3*: Indicates that all parameters adopt des_ecb3 encryption. *none*: Indicates cleartext transmission of all parameters.
Command Mode	Global configuration mode
Usage Guide	You can add or delete any parameter.

Configuration Example

↘ Configuring a Custom URL Format

Configuration Steps	● Configure redirection URL parameters including the user IP address, user MAC address, NAS IP address, SSID, and URL in cleartext.
	Hostname(config.tmplt.eportalv2)# fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl
Verification	● Check whether the configuration succeeds.
	Hostname(config)#show running-config ... fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl

1.4.14. Configuring the Redirection HTTP Port

Configuration Effect

- When an STA accesses network resources (for example, the user accesses the Internet using a browser), the STA sends HTTP packets. The NAS or convergence device intercepts these HTTP packets to determine

whether the STA is accessing network resources. If the NAS or convergence device detects that the STA is not authenticated, it prevents the STA from accessing network resources and displays an authentication page to the STA. By default, the NAS intercepts the HTTP packets that STAs send to port 80 to determine whether STAs are accessing network resources.

- After a redirection HTTP port is configured, the HTTP requests that STAs send to the specified destination port can be redirected.

Notes

- The commonly used management ports on the NAS or convergence device, such as ports 22, 23 and 53, and ports reserved by the system are not allowed to be configured as the redirection port. All ports except port 80 with numbers smaller than 1000 are seldom used by the HTTP protocol. To avoid a conflict with the well-known TCP port, do not configure a port with a small number as the redirection port unless necessary.

Configuration Steps

- Optional.
- When you configure automatic client acquisition, if you need to enable the NAS to intercept the HTTP packets that STAs send to the specified destination port, configure a redirection HTTP port.

Verification

- Configure an interception port.
- Open the browser of a PC and access the Internet through the port without performing authentication.
- Check whether the access requests are redirected to an authentication page.

Related Commands

↘ Configuring the Redirection HTTP Port

Command	**http redirect port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Global configuration mode
Usage Guide	A maximum of 10 different destination port numbers can be configured, not including default ports 80 and 443.

Configuration Example

↘ Configuring the Redirection HTTP Port

Configuration Steps	● Configure port 8080 as the redirection HTTP port.
	Hostname(config)#http redirect port 8080
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure port 8080 as the redirection HTTP port.
	Hostname(config)#http redirect port 8080
Verification	● Check whether the configuration is successful.
	Hostname(config)#show web-auth rdport Rd-Port: 80 443 8080

1.4.15. Configuring Rate Limit Webauth Logging

Configuration Effect

- The Web authentication module sends syslog messages to the administrator to display the information and relevant events of users who perform login/logout. By default, syslog messages are shielded.
- After syslog output rate limiting is configured, syslog messages are sent at a certain rate.

Notes

- When the login/logout rate is high, syslog messages are output frequently, which affects device performance and results in spamming.

Configuration Steps

- Optional.
- Configure syslog output rate limiting when you need to view the syslog messages about user login/logout.

Verification

- Configure logging rate limiting.
- Check whether users log in and out at a certain rate.
- Check that syslog messages are printed out at the limit rate.

Related Commands

↘ Configuring Rate Limit Webauth Logging

Command	**web-auth logging enable** *num*
Parameter Description	*num*: Indicates the syslog output rate (entry/second).
Command Mode	Global configuration mode
Usage Guide	When the syslog output rate is set to **0**, syslog messages are output without limit. The output of syslog messages of the critical level and syslog messages indicating errors is not limited.

Configuration Example

Configuring Rate Limit Webauth Logging

Configuration Steps	● Disable rate limit Webauth Logging.
	Hostname(config)#web-auth logging enable 0
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth logging enable 0 ...

1.4.16. Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Effect

- When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The NAS or convergence device intercepts the HTTP packets and redirects the user to a Web authentication page. To prevent an unauthenticated user from initiating too many HTTP connection requests and save resources on the NAS, it is necessary to limit the maximum number of HTTP sessions that the unauthenticated user can initiate on the NAS.
- A user occupies an HTTP session when performing authentication, and the other application programs of the user may also occupy HTTP sessions. For this reason, it is recommended that the maximum number of HTTP sessions for an unauthenticated user be not set to 1. By default, each unauthenticated user can initiate 255 HTTP sessions globally, and each port supports up to 300 HTTP sessions initiated by unauthenticated clients.

Notes

- If the authentication page fails to be displayed during Web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that may occupy HTTP sessions and then perform Web authentication again.

Configuration Steps

- Optional.
- Perform this configuration when you need to change the maximum number of HTTP sessions that each unauthenticated user can initiate and the maximum number of HTTP sessions that unauthenticated clients can initiate on each port.

- Perform this configuration when you configure automatic SU client acquisition.

Verification

- Modify the maximum number of HTTP sessions that an unauthenticated user can initiate.
- Simulate the scenario where an unauthenticated user constructs identical sessions to connect to the NAS continuously.
- Simulate the scenario where the unauthenticated user accesses the Internet using a browser. Check whether the access requests are redirected and the NAS notifies the user that the maximum number of sessions is reached.

Related Commands

↘ Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Command	**http redirect session-limit** { *session-num* }
Parameter Description	*session-num*: Indicates the maximum number of HTTP sessions for unauthenticated clients. The value range is 1 to 255. The default value is 255.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Steps	● Set the maximum number of HTTP sessions for unauthenticated clients to 3.
	Hostname(config)#http redirect session-limit 3
Verification	● Check whether the configuration is successful.
	Hostname(config)#show web-auth parameter HTTP redirection setting: session-limit: 3 timeout: 3 Hostname(config)#

1.4.17. Configuring the HTTP Redirection Timeout

Configuration Effect

- Configure the HTTP redirection timeout to maintain redirection connections. When an unauthenticated user tries to access network resources through HTTP, the TCP connection requests sent by the user will be intercepted and re-established with the NAS or convergence device. Then, the NAS or convergence device

waits for the HTTP GET/HEAD packets from the user and responds with HTTP redirection packets to close the connection. The redirection timeout is intended to prevent the user from occupying the TCP connection for a long time without sending GET/HEAD packets. By default, the timeout for maintaining a redirection connection is 3s.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to change the timeout for maintaining redirection connections.

Verification

- Change the timeout period.
- Use a network packet delivery tool to set up a TCP connection.
- View the status of the TCP connection on the NAS. Check whether the TCP connection is closed when the timeout is reached.

Related Commands

↘ Configuring the HTTP Redirection Timeout

Command	**http redirect timeout** { *seconds* }
Parameter Description	*Seconds*: Indicates the timeout for maintaining redirection connections, in the unit of seconds. The value ranges from 1 to 10. The default value is 3s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the HTTP Redirection Timeout

Configuration Steps	● Set the HTTP redirection timeout to 5s.
	Hostname(config)#http redirect timeout 5
Verification	● Check whether the configuration is successful.
	Hostname(config)#show web-auth parameter HTTP redirection setting: session-limit: 255 timeout: 5

1.4.18. Configuring the Authentication-Free Network Resource

Configuration Effect

- After Web authentication or 802.1Xauthentication is enabled on a port, the users connecting to the port need to pass Web authentication or 802.1Xauthentication before accessing network resources.
- Perform this configuration to exempt users from authentication when accessing some network resources.
- If a website is configured as a network resource of authentication exemption, all users, including unauthenticated clients, can access the website. By default, authentication exemption is not configured, and unauthenticated clients are not allowed to access network resources.
- IPv6 is supported.

Notes

- The maximum number of free resources and the maximum number of unauthenticated clients cannot exceed 1000 respectively. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be set.
- **http redirect direct-site** is used to configure the authentication-free URL address for users, and **http redirect** is used to configure the authentication-free IP address of the Web authentication server. The addresses configured using the two commands can be accessed without authentication, but they have different usages. It is recommended not to configure the IP address of the Web authentication server by using **http redirect direct-site**.
- When IPv6 addresses are used, you need to allow local link address learning. If this function is not configured, the NAS cannot learn the MAC addresses of clients.

Configuration Steps

- Optional.
- Run the **http redirect direct-site** command to enable unauthenticated clients to access network resources.

Verification

- Configure the authentication-free network resources.
- Check whether unauthenticated clients can access the configured network resources using PCs.

Related Commands

↘ Configuring the Authentication-Free Network Resources

Command	**http redirect direct-site** { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp**] | *mac-address* | range *starip-address endip-address* } [description *description-str*] [group *group-name*]
Parameter Description	*ipv6-address*: Indicates the IPv6 address of the authentication-free network. *ipv4-address*: Indicates the IPv4 address of the authentication-free network.

	ip-mask: Indicates the IPv4 subnet mask of the authentication-free network. *mac-address*: Indicates the MAC address of the authentication-free network. *startip-address:* Indicates the start IP address of the authentication-free network. *endip-address:* Indicates the end IP address of the authentication-free network. *group-name:* Indicates the group that the authentication-free network belongs to. *description-str:* Indicates the description about the authentication-free network.
Command Mode	Global configuration mode
Usage Guide	To set authentication-free ARP resource, use the **http redirect direct-arp** command preferentially.

Configuration Example

↘ Configuring the Authentication-Free Network Resources

Configuration Steps	● Configure the authentication-free network resources as 192.168.0.0/16.
	Hostname(config)#http redirect direct-site 192.168.0.0 255.255.0.0
	● Configure an authentication-free network from 10.0.0.1 to 12.0.0.1. Hostname (config)# http redirect direct-site range 10.0.0.1 12.0.0.1
Verification	● Check whether the configuration is successful.
	Hostname(config)#show web-auth direct-site Direct sites: Address Mask ARP Binding Group Description --- --- --- --- --- 192.168.0.0 255.255.0.0 Off N/A N/A Hostname(config)# Hostname(config)#show web-auth direct-site range Direct site Ranges: 1 Start Address End Address Group Description --- --- --- --- 10.0.0.1 12.0.0.1 N/A N/A Hostname(config)#

1.4.19. Configuring the Authentication-Free ARP Resource Range

Configuration Effect

When ARP check or similar functions are enabled, the ARP learning performed by clients is controlled. As a result, clients cannot learn the ARPs of the gateway and other devices, which affects user experience. You can configure the authentication-free ARP resource range to permit the ARP learning packets destined for the specified address to pass.

Notes

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the Layer-2 access device as a authentication-free ARP resource. Note the following point when you perform the configuration:
- When you configure authentication-free websites and ARP resources in the same address or network segment, the **http redirect direct-arp** command automatically combines the websites and ARP resources. If no ARP option is specified for the configured websites, an ARP option will be automatically added after the combination.
- When ARP check is enabled, if the outbound addresses of the PCs connecting to the Layer-2 access device are not the gateway address, configure the outbound addresses as authentication-free ARP resources. If multiple outbound addresses exist, configure these addresses as authentication-free ARP resources.

Configuration Steps

- Optional.
- If ARP check is enabled on the NAS, you must configure the free resources and gateway address as authentication-free ARP resources.

Verification

- Configure authentication-free ARP resources.
- Clear the ARP cache of the PC of an unauthenticated user. (Run the **arp -d** command in the Windows operating system.)
- Run the **ping** command on the PC to access the authentication-free ARP resources.
- View the ARP cache on the PC (run the **arp -a** command in the Windows operating system) and check whether the PC learns the ARP address of the authentication-free ARP resources.

Related Commands

↘ Configuring the Authentication-Free ARP Resource Range

Command	**http redirect direct-arp** {*ip-address* [*ip-mask*] }
Parameter Description	*ip-address*: Indicates the IP address of free resources. *ip-mask*: Indicates the mask of free resources.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Authentication-Free ARP Resource

Configuration Steps	● Configure the authentication-free ARP resource as 192.168.0.0/16.
	Hostname(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure the authentication-free ARP resource as 192.168.0.0/16.
	Hostname(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
Verification	● Check whether the configuration is successful.
	Hostname(config)#show web-auth direct-arp Direct arps: Address Mask --- --- 192.168.0.0 255.255.0.0 Hostname(config)#

1.4.20. Configuring an Authentication-Free Address Range

Configuration Effect

- Exempt users from Web authentication when accessing reachable network resources. By default, no authentication-free address range is configured. All users must pass Web authentication before accessing network resources.
- The authentication-free address range can be configured as an IP address range or MAC address range.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure an authentication-free user.
- Check whether the user can access the Internet without authentication.

Related Commands

↘ Configuring an Authentication-Free Address Range

Command	**web-auth direct-host** { *ipv4-address* [*ipv4-mask*] [**arp**] [**port** *interface-name*] | *ipv6-address* | *mac-address* | **range** *starip-address endip-address* } [**description** *description-str*] [**group** *group-name*] [**permit-ipv6**]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the user exempt from authentication.

	ipv6-address: Indicates the IPv6 address of the user exempt from authentication. *ipv4-mask*: Indicates the mask of the IPv4 address of the user exempt from authentication. *interface-name*: Indicates the name of the interface on which authentication exemption is enabled. *mac-address*: Indicates the MAC address of the user exempt from authentication. *startip-address:* Indicates the start IP address of authentication-free users. *endip-address:* Indicates the end IP address of authentication-free users. *group-name:* Indicates the group that the authentication-free users belong to. *description-str:* Indicates the description about the authentication-free users.
Command Mode	Global configuration mode
Usage Guide	The **arp** field is used to assign pass permissions to ARP packets. This field must be set when ARP check is enabled. After the **port** field is set, authentication exemption takes effect only on the configured interface.

Configuration Example

↘ Configuring an Authentication-Free Address Range

Configuration Steps	● Configure an authentication-free address range.
	Ruijie (config)# web-auth direct-host 192.168.197.64
	● Configure an authentication-free user range from 10.0.0.1 to 12.0.0.1. Hostname (config)# web-auth direct-host range 10.0.0.1 12.0.0.1
Verification	● Check whether the configuration is successful.
	Hostname(config)#show web-auth direct-host Direct hosts: Address Mask Port ARP Binding Group Description --- --- --- --- --- --- 192.168.197.64 255.255.255.255 Off N/A N/A Hostname(config)# Hostname# show web-auth direct-host range Direct host Ranges: 1 Start Address End Address Port Group Description --- --- --- --- --- 10.0.0.1 12.0.0.1 Gi0/2 N/A N/A

1.4.21. Configuring the Interval for Updating Online User Information

Configuration Effect

- The NAS or convergence device maintains and periodically updates the information of online users, including users' online duration, to monitor the usage of network resources. When the online duration threshold is reached, users will be prevented from using network resources.

Notes

- The user information updating interval must be configured as 60 or multiple of 60; otherwise, the system will select the minimum multiple of 60 above and closest to the actual configuration as the interval.

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure the interval for updating online user information.
- View the information of online users after the update interval has elapsed.

Related Commands

↘ Configuring the Interval for Updating Online User Information

Command	**web-auth update-interval** *{ seconds }*
Parameter Description	*seconds*: Indicates the interval for updating online user information, in the unit of seconds. The value ranges from 30 to 3,600. The default value is 180s.
Command Mode	Global configuration mode
Usage Guide	To restore the default updating interval, run the **no web-auth update-interval** command in global configuration mode.

Configuration Example

↘ Configuring the Interval for Updating Online User Information

Configuration Steps	● Set the interval for updating online user information to 60s.
	Ruijie (config)# web-auth update-interval 60
Verification	● Check whether the configuration is successful.
	Hostname(config)#show run | include web-auth update-interval web-auth update-interval 60

1.4.22. Configuring Portal Detection

Configuration Effect

- Detect the availability of the active portal server periodically. When the active portal server is unavailable, the standby portal server takes over the services.

- Ruijie Second-Generation Web Authentication provides two detection methods. One is that the NAS constructs and sends portal packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Another is the NAS sends ping packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Because some servers or intermediate network segments filter ping packets, the first method is commonly used. The ping detection method is only used based on special requirements. In Ruijie First-Generation Web Authentication, the NAS connects to a port of the portal server and checks whether the port is reachable. If the portal is reachable, the NAS determines that the portal server is available.
- For the first method in the second-generation authentication, the interval of server availability detection is specified by the **interval** parameter, and the maximum number of packets that can be sent during each time of detection is specified by the **retransmit** parameter. If the portal server does not respond, the NAS determines that the portal server is unavailable. The timeout period for each packet is specified by the **timeout** parameter. The parameter settings are also supported by Ruijie First-Generation Web Authentication.
- Portal server detection takes effect for Ruijie First- and Second-Generation Web Authentication.
- If multiple portal servers are configured, these servers are working in active/standby mode.

Notes

- Multiple portal servers must be configured to realize failover when an error is detected on one server.
- Only one of the two detection methods can be used at a time in case of collision. If both detection methods are configured, a detection algorithm conflict will occur or the detection results will be inaccurate.
- The system will automatically select a detection method based on whether Ruijie First- or Second-Generation Web Authentication is used.

Configuration Steps

- Optional.
- Configure multiple portal server templates applicable to Ruijie First- or Second-Generation Web Authentication.

Verification

- Configure two portal server templates for Ruijie First- or Second-Generation Web Authentication. Make the first template point to an unavailable server and the second template point to an available server.
- When the Console displays a log indicating that the portal server is not available, simulate the scenario where a user opens a browser to perform login authentication. Check whether the user is redirected to the second portal server.

Command	**web-auth portal-check** [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries]
Parameter Description	*intsec*: Indicates the detection interval. The default value is 10s. *tosec:* Indicates the packet timeout period. The default value is 5s. *intsec*: Indicates the timeout retransmission times. The default value is 3 (times).
Command Mode	Global configuration mode

Usage Guide	In many network environments, only one portal server is deployed, and portal server detection does not need to be configured. If multiple portal servers exist, it is recommended that the parameters of portal server detection be not set to small values; otherwise, the NAS will send many packets within a short time, affecting performance. This command cannot be used together with the **fmt** command. To use the **fmt** command to configure the URL format, run the **web-auth ping** command to perform Portal inspection.
Command	**web-auth ping** [**interval** *minutes* | **retry** *times*]
Parameter Description	*minutes*: Indicates the detection interval. The default value is 1 minute. *times*: Indicates the timeout retransmission times. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	In many network environments, only one portal server is deployed, and portal server detection does not need to be configured. If multiple portal servers exist, it is recommended that the parameters of portal server detection be not set to small values; otherwise, the NAS will send many packets within a short time, affecting performance. This command must be used together with the **fmt** command. Before using this command, run the **fmt** command to configure the URL format. Otherwise, this command does not take effect.

Configuration Example

↘ Configuring Portal Detection

Configuration Steps	● Configure portal detection.
	Hostname(config)#web-auth portal-check interval 20 timeout 2 retransmit 2
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth portal-check interval 20 timeout 2 retransmit 2 ...

1.4.23. Configuring Portal Escape

Configuration Effect

- Allow new users to access the Internet without authentication when the portal server is not available.

Notes

- To use the portal escape function, you must configure portal detection.

- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are not available.
- The escape function is intended only for the portal server, instead of the RADIUS server.

Configuration Steps

- Optional.
- Configure portal detection.
- Configure portal escape.
- (Optional) Configure the nokick attribute.

Verification

- Configure a portal server and disable the server.
- Configure the portal detection and escape functions.
- When the NAS detects that the portal server is not available, check whether a client accesses the Internet without authentication.

Related Commands

↘ Configuring Portal Escape

Command	web-auth portal-escape [nokick]
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure portal escape if the continuity of some critical services on the network needs to be maintained when the portal server is faulty. You must configure portal detection when you use this function. If the nokick attribute is configured, the system does not force users offline when the escape function takes effect. If the nokick attribute is deleted, the system forces users offline.

Configuration Example

↘ Configuring Portal Escape

Configuration Steps	● Configure portal escape.
	Hostname(config)#web-auth portal-escape
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth portal-escape

Configuration Steps	● Configure portal escape.
	Hostname(config)#web-auth portal-escape
Verification	● Check whether the configuration is successful.
	...

1.4.24. Enabling DHCP Address Check

Configuration Effect

- Allow only the clients that are allocated with IP addresses through DHCP to perform authentication.

Notes

- To use the DHCP address check function, you must configure DHCP snooping.
- DHCP address check is supported only for IPv4.
- DHCP address check is applicable only to Ruijie Second-Generation Web Authentication and iPortal Web Authentication.
- The requirement that users obtain IP addresses through DHCP must be specified during network deployment. Those users cannot also use static IP addresses; otherwise, the existing users that use static IP addresses will be affected.
- If a few users need to use static IP addresses, configure these IP addresses as authentication-free addresses, and these users are exempt from authentication.
- If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable the global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled in each interface.

Configuration Steps

- Optional.
- Enable DHCP snooping.
- Enable DHCP address check.

Verification

- Enable DHCP address check.
- Configure a static IP address that is not allocated by the DHCP server on a client.
- Connect the client to the Internet and check whether the STA cannot perform authentication.

Related Commands

↘ **Enabling Global DHCP Address Check**

Command	web-auth dhcp-check
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure DHCP address check to allow only the users who obtain IP addresses through DHCP to access the Internet. This function helps prevent the users who configure IP addresses without authorization from performing authentication to access the Internet.

Configuration Example

↘ Enabling DHCP Address Check

Configuration Steps	● Enable global DHCP address check.
	Hostname(config)#web-auth dhcp-check
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth dhcp-check ... interface TenGigabitEthernet 3/1 web-auth dhcp-check vlan 1,3-4 ...

1.4.25. Disabling Link Detection

Configuration Effect

- The authentication entries of clients are kept when links are disconnected. The clients can access the Internet again without authentication if the IP addresses remain unchanged.
- You can disable link detection in places where mobile office is required or wireless Web authentication is deployed but wireless signal is bad.

Notes

- Do not disable link detection if clients obtain IP addresses through DHCP and the number of IP addresses in the DHCP address pool is smaller than the number of clients. If link detection is disabled, the IP address of a client that has logged out may be obtained by another client, causing a user information error.
- If link detection is disabled, a client logout action is triggered only when the user clicks the **Logout** button on the online page, the server forces the client offline, or the NAS detects low traffic on the client. It is

recommended that you enable low traffic detection if you need to disable link detection. For details, see the *Configuring SCC*.

- It is recommended that you disable link detection and enable low traffic detection in a wireless environment. The reason is that the offline rate in a wireless environment is high because wireless connections are easily affected by signal interference, and disabling link detection helps improve wireless experience.

Configuration Steps

- Optional.
- Configure Web authentication.
- Disable link detection.

Verification

- Configure Ruijie-Second Generation Web Authentication and disable link detection.
- Connect a client to the Internet and perform authentication. When the client passes the authentication, disconnect from and then reconnect to the Internet with the same IP address. Check whether the client can access the Internet again without authentication.

Related Commands

↘ Disabling Link Detection

Command	**no web-auth sta-leave detection**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can disable link detection in a wireless environment or a wired environment with the need for mobile office. To disable link detection, you must enable low traffic detection.

Configuration Example

↘ Disabling Link Detection

Configuration Steps	● Disable link detection.
	Hostname(config)#no web-auth sta-leave detection
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... no web-auth sta-leave detection ...

1.4.26. Disabling Portal Extension

Configuration Effect

- Enable portal extension to support Ruijie portal server and portal servers that comply with the CMCC WLAN Service Portal Specification.
- You can select multiple redirection URL formats when interworking with the servers comply with the CMCC WLAN Service Portal Specification to achieve compatibility with different servers.

Notes

- Only Ruijie Second-Generation Web Authentication supports portal extension.
- Ruijie Second-Generation Web Authentication extends the CMCC WLAN Service Portal Specification. You need to determine whether to use the extension mode based on the server performance.
- If the portal server is a product of Ruijie, use the default mode, that is, extension mode. If the portal server complies with the CMCC WLAN Service Portal Specification, disable portal extension.
- The CMCC WLAN Service Portal Specification supports multiple redirection URL formats. If the portal server complies with the CMCC WLAN Service Portal Specification, select a redirection URL format supported by the server.

Configuration Steps

- Optional.
- Determine whether to disable portal extension based on the server type.
- Select a redirection URL format supported by the server if portal extension is disabled.

Verification

- Select Ruijie portal server and a portal server compliant with the CMCC WLAN Service Portal Specification to be used in Ruijie Second-Generation Web Authentication.
- Connect a client to the Internet. Check whether the client performs authentication normally on the two servers and can access the Internet.

Related Commands

↘ Disabling Portal Extension

Command	**no web-auth portal extension**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The portal servers that comply with the *CMCC WLAN Service Portal Specification* are deployed. If Ruijie portal server is used, enable portal extension.

Configuration Example

↘ Disabling Portal Extension

Configuration Steps	● Disable portal extension.
	Hostname(config)#no web-auth web-auth portal extension
	Hostname(config)# http redirect url-fmt ext1
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... no web-auth web-auth portal extension http redirect url-fmt ext1 ...

1.4.27. Configuring a Whitelist and Blacklist

Configuration Effect

- Configure a whitelist to allow unauthenticated clients to access some network resources, and configure a blacklist to prevent authenticated clients from accessing some network resources.
- Blacklists and whitelists are supported based on ports, URLs, and IP addresses.

Notes

- Up to 1,000 blacklists and whitelists can be configured.
- If blacklists and whitelists are configured in the domain name format, the DNS function must be configured on the NAS so that the NAS can resolve IP addresses correctly.
- A domain name can map up to eight IP addresses.

Configuration Steps

- Optional.
- Configure DNS.
- Configure a whitelist and blacklist.

Verification

- Configure a whitelist and blacklist.
- Check whether unauthenticated STAs can access the whitelisted addresses.
- Check whether authenticated STAs cannot access the blacklisted addresses.

Related Commands

Configuring a Whitelist and Blacklist

Command	**web-auth acl { black-ip** *ip* **| black-port** *port* **| black-url** *name* **| white-url** *name* **}**
Parameter Description	*ip*: Indicates an IP addresses blacklisted. *port*: Indicates a port numbers blacklisted. *name*: Indicates a URL blacklisted or whitelisted.
Command Mode	Global configuration mode (Blacklists can be configured in WLAN security configuration mode on wireless devices.)
Usage Guide	Configure a whitelist to allow unauthenticated clients to access some network resources, and configure a blacklist to prevent authenticated clients from accessing some network resources.

Configuration Example

Configuring a Whitelist and Blacklist

Configuration Steps	● Configure a whitelist and blacklist.
	Hostname(config)#web-auth acl black-ip 192.168.1.2 Hostname(config)#web-auth acl white-url www.host.com
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth acl black-ip 192.168.1.2 web-auth acl white-url www.host.com ...

1.4.28. Configuring Jitter-off Accounting

Configuration Effect

- If jitter-off or low traffic detection is configured on the NAS, the time of jitter-off or low traffic detection will be accounted into the online duration. Jitter-off accounting is used to reduce the accounting error. Configure this function if the accounting policy does not allow the deduction of the anti-jitter time or low traffic detection time from the online duration.

Notes

- The NAS needs to support anti-jitter or low traffic detection.

- A client logs out for the link is disconnected for a long time or the NAS detects its low traffic.
- When the jitter-off and low traffic detection functions are enabled, the first logout is accounted with jitter-off time only. For example, the jitter-off duration is set to 5 minutes and the low traffic detection duration is set to 10 minutes; if the client is disconnected from the network, the jitter-off function first triggers Web authentication to log the client out. In this case, only the5-minute duration is deducted from the online duration in the accounting packet.

Configuration Steps

- Optional.
- Configure the accounting function.
- Configure jitter-off or low traffic detection.
- Configure jitter-off accounting.

Verification

- Simulate the scenario where a client goes online after authentication and then offline because the low traffic threshold is reached.
- Capture the stop-accounting packet sent by the NAS and check whether the time of low traffic detection is deducted from the online duration.

Related Commands

Configuring Jitter-off Accounting

Command	**web-auth accounting jitter-off**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to include the jitter-off duration or low traffic detection time into the online duration in the stop-accounting packet based on the server accounting policy. By default, they are not included.

Configuration Example

Configuring Jitter-off Accounting

Configuration Steps	• Configure jitter-off accounting.
	Hostname(config)#web-auth accounting jitter-off
Verification	• Check whether the configuration is successful.
	Hostname(config)#show running-config ...

Configuration Steps	● Configure jitter-off accounting.
	Hostname(config)#web-auth accounting jitter-off
Verification	● Check whether the configuration is successful.
	web-auth accounting jitter-off ...

1.4.29. Configuring the Portal Communication Port

Configuration Effect

- Configure the port (source port) used for the communication between the NAS and portal server.

Notes

- Only one port can be configured for the communication between the NAS and portal server.

Configuration Steps

- Configure a port as the portal communication port.

Verification

- After Web authentication is enabled, capture a packet on the portal server during the authentication process and check whether the source IP address of the packet is the IP address of the specified port.

Related Commands

↘ Configuring the Portal Communication Port

Command	**ip portal source-interface** *interface-type interface-num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Portal Communication Port

Configuration Steps	● Configure an aggregate port as the portal communication port.
	Hostname(config)#ip portal source-interface Aggregateport 1

Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ip portal source-interface Aggregateport 1

1.4.30. Configuring a NDKEY-Compatible Webauth URL

Configuration Effect

- Configure the Webauth URL used in Web authentication to support the Shanghai NDKEY system.

Notes

- N/A

Configuration Steps

↘ Configuring a NDKEY-Compatible Webauth URL

- Set the post parameter in global configuration mode.

Command	**web-auth dkey-compatible url-parameter** *string*
Parameter Description	*string*: Indicates the value of the **post** parameter.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Execute redirection after the configuration and check that the redirection URL contains the post parameter.

Configuration Example

↘ Configuring Noise Reduction Suppression

Configuration Steps	● Configure compatibility parameters.
	Hostname(config)#web-auth dkey-compatible url-parameter login
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config

Configuration Steps	● Configure compatibility parameters.
	Hostname(config)#web-auth dkey-compatible url-parameter login
Verification	● Check whether the configuration is successful.
	... web-auth dkey-compatible url-parameter login

1.4.31. Enabling NAT for Ruijie iPortal Web Authentication

Configuration Effect

- Configure Ruijie iPortal Web Authentication to support NAT.

Notes

- NAT takes effect only in Ruijie iPortal Web Authentication.

Configuration Steps

↘ Enabling NAT for Ruijie iPortal Web Authentication

- Enable NAT in global configuration mode.

Command	**iportal nat enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check whether Ruijie iPortal Web Authentication can be implemented after NAT is enabled.

Configuration Example

↘ Enabling NAT for Ruijie iPortal Web Authentication

Configuration Steps	● Enable NAT for Ruijie iPortal Web Authentication.
	Hostname(config)#iportal nat enable

Verification	• Check whether the configuration is successful.
	Hostname(config)#show running-config ... iportal nat enable

1.4.32. Configuring the iPortal HTTP Retransmission Times

Configuration Effect

- Configure the iPortal HTTP retransmission times.

Notes

- The retransmission times configuration takes effect only for the HTTP connections pushed by an iPortal page.

Configuration Steps

↘ Configuring the iPortal HTTP Retransmission Times

- Set a parameter in global configuration mode.

Command	**iportal retransmit** *count*
Parameter Description	*count*: Indicates the retransmission times.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Send an iPortal Web authentication request and disconnect from the network. Check whether the NAS resends an HTTP connection request.

Configuration Example

↘ Configuring the Retransmission Times

Configuration Steps	• Configure the retransmission times.
	Hostname(config)#iportal retransmit 5
Verification	• Check whether the configuration is successful.

Configuration Steps	● Configure the retransmission times.
	Hostname(config)#iportal retransmit 5
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... iportal retransmit 5

1.4.33. Configuring Service Selection in Ruijie iPortal Web Authentication

Configuration Effect

- Configure the service type used by Ruijie iPortal Web Authentication.

Notes

- N/A

Configuration Steps

↘ Configuring the Service Type Used by Ruijie iPortal Web Authentication

- Configure a service type in global configuration mode.

Command	**iportal service [internet** *internet-name* | **local** *local-name* **]**
Parameter Description	*internet-name*: Indicates the external service name to be used. *local-name*: Indicates the internal service name to be used.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring a Service Type

Configuration Steps	● Configure a service type.
	Hostname(config)#iportal service local local-srv
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure a service type.
	Hostname(config)#iportal service local local-srv
Verification	● Check whether the configuration is successful.
	Hostname(config)#show running-config ... iportalservice local local-srv

1.4.34. Configuring the Accounting Method List of Web Authentication

Configuration Effect

- Configure Web authentication accounting methods based on different WLANs.

Notes

- If no accounting method is configured for Web authentication, the default method is used.

Configuration Steps

↘ Configuring an Accounting Method

Command	**web-auth accounting v2 { default | *name* }**
Parameter Description	*name*: Indicates the name of the accounting method list to be used.
Command Mode	Global configuration mode\WLAN security configuration mode
Usage Guide	N/A

Verification

- View the destination IP address of accounting packets.

Configuration Example

↘ Configuring an Accounting Method

Configuration Steps	● Configure an accounting method.
	Hostname(config.tmplt.eportalv2)#web-auth accounting v2 default

Verification	• Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth accounting v2 default

1.4.35. Configuring a Web Authentication Method List

Configuration Effect

- Configure Web authentication methods based on different templates.

Notes

- If no Web authentication method is configured, the default method is used.

Configuration Steps

↘ Configuring a Web Authentication Method List

Command	**web-auth authentication v2 { default |** *name* **}**
Parameter Description	*name*: Indicates the name of the Web authentication method list to be used.
Command Mode	Global configuration mode\WLAN security configuration mode
Usage Guide	N/A

Verification

- View the destination IP address of authentication packets.

Configuration Example

↘ Configuring a Web Authentication Method

Configuration Steps	• Configure a Web authentication method.
	Hostname(config.tmplt.eportalv2)#web-auth authentication v2 default
Verification	• Check whether the configuration is successful.
	Hostname(config)#show running-config ... web-auth authentication v2 default

1.4.36. Configuring a Delay for Users to Go Offline Upon Interface Down

Configuration Effect

- After this command is configured, users will not go offline immediately upon interface Down. Instead, users will stay online for a period before logout.

Notes

- N/A

Configuration Steps

↘ Configuring a Delay for Users to Go Offline Upon Interface Down

- Configure this function in global configuration mode.

Command	**web-auth linkdown-timeout** *timeout*
Parameter Description	Indicates a delay for users to go offline upon interface Down in seconds. The default is 60.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- After the interface becomes Down, the user goes offline when the configured timer expires.

Configuration Example

↘ Configuring a Delay for Users to Go Offline Upon Interface Down

Configuration Steps	• Configure a delay for users to go offline upon interface Down. Hostname(config)# web-auth linkdown-timeout 10
Verification	• Check whether the configuration succeeds. Hostname(config)#show running-config

1.4.37. Configuring RADIUS Authentication Escape

Configuration Effect

- After RADIUS authentication escape is enabled, web users can still perform authentication to access the Internet in the case of a RADIUS server failure.

Notes

- This function must be used together with RADIUS server detection command.

Configuration Steps

Configuring RADIUS Authentication Escape

Command	web-auth radius-escape
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- After configuring RADIUS server detection, use an inaccurate username and password to pass the authentication in the case of a RADISU server failure.

Configuration Example

Configuring RADISU Authentication Escape

Configuration Steps	• Enable RADIUS authentication escape. Hostname(config)# web-auth radius-escape
Verification	• Check whether the configuration succeeds. Hostname(config)#show running-config

1.4.38. Configuring Noise Reduction in Wireless Web Authentication

Configuration Effect

- When the number of times an STA accesses an IP address reaches the configured threshold, the subsequent packets that the STA sends to the IP address will be dropped, in order to realize noise reduction.

Notes

- Configure the two parameters (aging time and hit times) for noise reduction based on the network condition and actual requirements to avoid the dropping of normal packets, which will affect redirection.

Configuration Steps

Configuring Noise Reduction in Global Configuration Mode

Command	**web-auth noise**[**aging** *agmin*] [**hit** *times*]
Parameter Description	*agmin*: Indicates the aging time of noise reduction. The default value is 1 minute. *times*: Is a rule of noise reduction. When the number of times an STA accesses an IP address reaches the threshold specified by the *times* parameter, noise is considered to occur. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Simulate the scenario where an STA accesses an IP address repeatedly during redirection until the maximum number of access times is reached. Check whether the subsequent packets that the STA sends to the IP address are redirected or not. After the aging time of the noise reduction has elapsed, check whether the packets that the STA sends to the IP address are redirected again.

Configuration Example

↘ Configuring Noise Reduction in Wireless Web Authentication

Configuration Steps	● Set the parameters of noise reduction in wireless Web authentication. Hostname(config)#web-auth noise aging 1 hit 3
Verification	● Check whether the configuration is successful. Hostname(config)#show running-config

1.4.39. Enabling iOS Automatic Pop-up Window Control in WeChat-Based Authentication

Configuration Effect

- Enable iOS STAs to support the automatic display of pop-up windows and display Wi-Fi signal reception during WeChat-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). (iOS STAs can use the WeChat app without login when the WeChat traffic authentication-free function is enabled.)

Notes

- iOS automatic pop-up window control must be used together with the WeChat traffic authentication-free function (run the web-ctrl free-auth weixin command to enable this function).
- The redirection performance will be reduced after iOS automatic pop-up window control is enabled.

- iOS automatic pop-up window control will be invalid when the authentication-free function is enabled for the Apple Inc. website by running the following commands:
- web-ctrl free-auth iphone
- web-auth acl white-url http://www.apple.com.cn
- web-auth acl white-url http://captive.apple.com

Configuration Steps

↘ Enabling iOS Automatic Pop-up Window Control in Global Configuration Mode

Command	http redirect adapter ios
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check that iOS STAs show pop-up windows and display Wi-Fi signal reception during WeChat-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). (iOS STAs can use the WeChat app without login when the WeChat traffic authentication-free function is enabled.)

Configuration Example

↘ Enabling iOS Automatic Pop-up Window Control in WeChat-Based Authentication

Configuration Steps	• Enable iOS automatic pop-up window control. • (Optional) The configuration is valid for the WeChat authentication scenario (configured with the **web-ctrl free-auth weixin** command). Hostname(config)#http redirect adapter ios
Verification	• Check whether the configuration is successful. Hostname(config)#show running-config

1.4.40. Enabling the Smart WeChat Web Authentication

Configuration Effect

- When an STA is associated with an SSID for the second time during WeChat Web authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication), the STA gets online without authentication.

Notes

- You need to run the ip dhcp snooping command before the smart authentication function takes effect.

Configuration Steps

↘ Configuring the Smart Authentication in Global Configuration Mode

Command	**web-auth sta-perception enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Simulate the scenario where an STA is associated with an SSID for the second time during WeChat Web authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). Check whether the STA gets online without authentication.

Configuration Example

↘ Enabling the Smart WeChat Web Authentication

Configuration Steps	• Enable the smart WeChat Web authentication. • The configuration is optional.
	Hostname(config)#web-auth sta-perception enable
Verification	• Check whether the configuration is successful.
	Hostname(config)#show running-config

1.4.41. Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol

Configuration Effect

- Configure transparent transmission of the 0x05 attribute of the portal protocol. After this function is enabled, the Web authentication server supports transparent transmission of the 0x05 attribute in the following scenarios:

1. When the portal protocol of China Mobile is interworked, the Web authentication server encapsulates the error flag into the 0x05 attribute (ErrID) and transparently transmits it to the portal server.
2. When Huawei portal protocol 2.0 is interworked, the Web authentication server encapsulates prompts from third-party authentication device such as the RADIUS server to the 0x05 attribute (TextInfo) and transparently transmits them to the portal server.

Notes

- This function is disabled by default.

Configuration Steps

- Optional.
- Configure this function when the ErrID (0x05) attribute specified in the portal protocol of China Mobile is required.
- Configure this function when the TextInfo (0x05) attribute specified in Huawei portal protocol 2.0 is required.

Related Commands

Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol in Global Configuration Mode

Command	**web-auth portal-attribute 5**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In general, enable this function on the portal server when a device needs to upload the error flag (ErrID).
Command	**web-auth portal-attribute textinfo**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In general, enable this function on the portal server (using Huawei portal protocol 2.0) when a device needs to upload prompts (TextInfo) from a third-party authentication device such as the RADIUS server.

Verification

- After this function is enabled, check that the 0x05 attribute is contained in the ACK packet responded to the portal server.

Configuration Example

Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol

Configuration Steps	● Configure transparent transmission of the 0x05 attribute. Hostname(config)# web-auth portal-attribute 5 Or: Hostname(config)# web-auth portal-attribute textinfo
Verification	● Check whether the configuration is successful. Hostname(config)#show running-config

1.4.42. Configuring Uniqueness Check of Portal Authentication Accounts

Configuration Effect

- Configure the uniqueness check of portal authentication accounts. After this function is enabled, the Web authentication server checks account information in the user authentication request. If finding that the account has been used by another user and is online, the Web authentication server directly responds to the portal server with ErrCode 2-contained ACK_AUTH. After receiving such response, some portal servers push the "Terminal Preemption" prompt to users.

Notes

- This function is disabled by default.

Configuration Steps

- Optional.
- Configure the function when the portal server needs to push the "Terminal Preemption" prompt to users.

Related Commands

↘ Configuring Uniqueness Check of Portal Authentication Accounts in Global Configuration Mode

Command	**web-auth portal-valid unique-name**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In general, configure the function when the portal server needs to push the "Terminal Preemption" prompt to users.

Verification

- After this function is enabled, if finding that a same account is used by another user and is online, the Web authentication server directly responds to the portal server with ErrCode 2-contained ACK_AUTH.

Related Commands

Configuring Uniqueness Check of Portal Authentication Accounts

Configuration Steps	● Configure uniqueness check of portal authentication accounts. Hostname(config)# web-auth portal-valid unique-name
Verification	● Check whether the configuration is successful. Hostname(config)#show running-config

1.4.43. Enabling the One-click Switch Configuration via WiFiDog

Configuration Effect

- Use one command to configure WiFiDog template information, port control, global survival, iOS window display, and imperceptible authentication.

Notes

- The **no** form of this command can delete template information and controlled ports, but is not globally valid.

Configuration Steps

Enabling the One-click Switch Configuration via WiFiDog

- Optional.

Command	**web-auth wifidog-template** *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* **url** *url-string* [**gateway-id** *gwid-string*] [**perception**]
Parameter Description	*name*: Indicates the template name. *wlanid-start*:Indicates the start WLAN ID. *wlanid-end*:Indicates the end WLAN ID. *portal-ip-addr*: Indicates the IP address of the portal server. *nas-ip-addr:* Sets the IP address for a device with WiFiDog configured to access a service, so that the server sends packets to this IP address for communication. *url-string:* Indicates the URL for portal server authentication. *gwid-string*: Applies to the hot standby or VAC scenario, which is often the serial number of the active AC. It is not required by the standalone scenario. **Perception**: Configures MAC Bypass.
Command Mode	Global configuration mode
Usage Guide	The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete

	template information and all the controlled ports, but is not globally valid.

Verification

- Run the **show running** command to check whether the configuration is normal.

Configuration Example

Enabling the One-click Switch Configuration via WiFiDog

Configuration Steps	● Enable the one-click switch configuration via WiFiDog.
	Hostname(config)# web-auth wifidog-template aaa wlan-range 2 5 portal-ip 172.21.6.78 nas-ip 192.168.197.227 url http://172.21.6.78/auth/wifidogAuth
Verification	● Run the **show running-config** command to check whether the configuration is successful.

1.4.44. Enabling the One-click Switch Configuration via WeChat

Configuration Effect

- Use one command to configure WeChat template information, port control, global survival, PC free authentication, iOS window display, and imperceptible authentication.

Notes

- The **no** form of this command can delete template information and controlled ports, but is not globally valid.

Configuration Steps

Enabling the One-click Switch Configuration via WeChat

- Optional.

Command	**web-auth wechat-template** *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* [**nas-id** *nas-id-string* **]** [**perception** | **ios-adapter**]
Parameter Description	*name*: Indicates the template name. *wlanid-start*: Indicates the start WLAN ID. *wlanid-end*: Indicates the end WLAN ID. *portal-ip-addr*: Indicates the IP address of the portal server. *nas-ip-addr:* Sets the IP address for a device with WeChat configured to access a service, so that the server sends packets to this IP address for communication. *nas-id-string*: Applied to the hot standby or VAC scenario, which is often the serial number of the active AC. It is not required in standalone scenarios. **Perception**: Configures MAC Bypass. **ios-adapter**: Configures the automatic popup window.

Command Mode	Global configuration mode
Usage Guide	The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.

Verification

- Run the **show running** command to check whether the configuration is normal.

Configuration Example

↘ Enabling the One-click Switch Configuration via WeChat

Configuration Steps	• Enable the one-click switch configuration via WeChat.
	Hostname(config)# web-auth wechat-template aaa wlan-range 2 5 portal-ip 172.21.6.78 nas-ip 192.168.197.227
Verification	• Run the **show running-config** command to check whether the configuration is successful.

1.4.45. Enabling the Device to Automatically Add a Domain Name to the Authentication Username

Configuration Effect

- If 2-nd generation Portal authentication and internal Portal authentication is configured with a domain name in the template, the domain name will be automatically added to the authentication username and sent to the AAA server.

Notes

- A domain name contains up to 63 bytes. The domain name is directly added to the username from the Portal server. If the new username consisting of the original username and the domain name exceeds 253 bytes, the exceeding part will be truncated.

Configuration Steps

- Optional.
- The Portal server does not add the domain name to the authentication username by default. If the domain name is required by the RADIUS server, configure this function.

Verification

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

Related Commands

Configuring the Device to Add a Domain Name to the Authentication Username

Command	**domain** *domain-string*
Parameter Description	*domain-string:* Indicates the domain name to be added.
Command Mode	Web authentication template configuration mode
Usage Guide	The authentication userame from the Portal server is **host**. After you configure domain name **@wifi**, the username sent to the RADIUS server is **host@wifi**.

Configuration Example

Configuring the Device to Automatically Add a Domain Name to the Authentication Username

Configuration Steps	● Configure automatic adding of domain name **@wifi** to the eportalv2 template.
	Hostname(config.tmplt.eportalv2)#domain @wifi
Verification	● Check whether the configuration succeeds. Hostname(config)#show run web-auth template eportalv2 domain @wifi Hostname(config)#

1.5. Monitoring

Clearing

Description	Command
Forces users offline.	**clear web-auth user** { **all** | **ip** *ip-address* | **ipv6** *ipv6-address* | **mac** *mac-address* | **name** *name-string* }
Clears all the authentication-free network resources.	**clear web-auth direct-site**
Clears all the authentication-free users.	**clear web-auth direct-host**
Clears the Webauth blacklist and whitelist configuration.	**clear web-auth acl**
Deletes all authentication-free ARP resources.	**clear web-auth direct-arp**

Displaying

Description	Command

Description	Command
Displays the Webauth blacklist and whitelist configuration.	**show web-auth acl**
Displays the basic parameters of Web authentication.	**show web-auth parameter**
Displays the Webauth template configuration.	**show web-auth template**
Displays the authentication-free host range.	**show web-auth direct-host**
Displays the authentication-free address range.	**show web-auth direct-site**
Displays the authentication-free ARP range.	**show web-auth direct-arp**
Displays the TCP interception port.	**show web-auth rdport**
Displays the Webauth configuration on a port.	**show web-auth control**
Displays the online information of all users or specified users.	**show web-auth user**{ **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **escape** }
Displays the Webauth portal check information.	**show web-auth portal-check**
Displays the noise reduction configuration of Web authentication.	**show web-auth noise**
Displays user login and logout records.	**show web-auth syslog ip** *ip-address*

Debugging

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

Description	Command
Debugs Web authentication.	**debug web-auth all**

1 Configuring SCC

1.1 Overview

The Security Control Center (SCC) provides common configuration methods and policy integration for various access control and network security services, so that these access control and network security services can coexist on one device to meet diversified access and security control requirements in various scenarios.

Typical access control services are dot1x, Web authentication, Address Resolution Protocol (ARP) check, and IP Source Guard. The network security services include Access Control List (ACL), Network Foundation Protection Policy (NFPP), and anti-ARP gateway spoofing. When two or more access control or network security services are simultaneously enabled on the device, or when both access control and network security services are simultaneously enabled on the device, the SCC coordinates the coexistence of these services according to relevant policies.

For details about the access control and network security services, see the related configuration guide. This document describes the SCC only.

Protocol and Standards

N/A

1.2 Application

Typical Application	Scenario
Access Control of Extended Layer 2 Campus Networks	Students on a campus network can access the Internet based on dot1x client authentication or Web authentication. ARP spoofing between the students should be prevented. In addition, terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

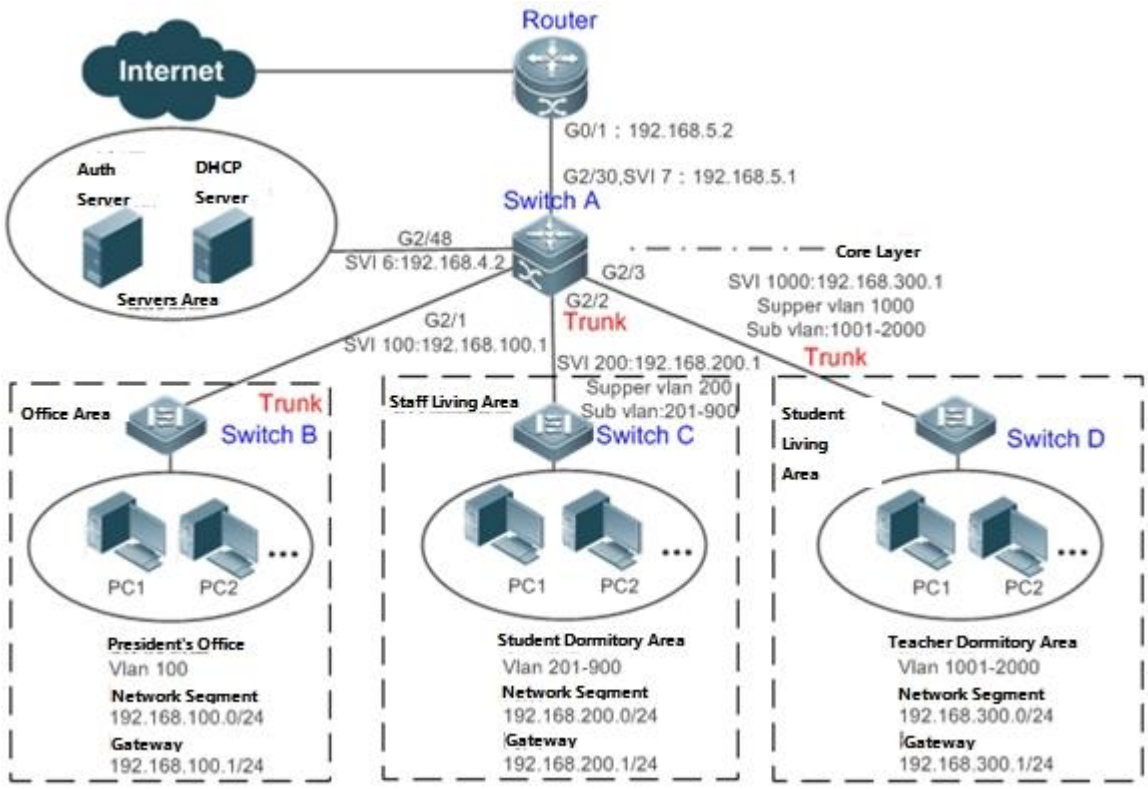
1.2.1 Access Control of Extended Layer 2 Campus Networks

Scenario

Students on a campus network of a university usually need to be authenticated through the dot1x client or Web before accessing the Internet, so as to facilitate accounting and guarantee the benefits of the university.

- The students can access the Internet through dot1x client authentication or Web authentication.
- ARP spoofing between the students is prevented, so as to guarantee the stability of the network.
- Terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

Figure 1-1



Remarks	A traditional campus network is hierarchically designed, which consists of an access layer, a convergence layer and a core layer, where the access layer performs user access control. On an extended Layer 2 campus network, however, user access control is performed by a core switch, below which access switches exist without involving any convergence device in between. The ports between the core switch and the access switches (such as switches B, C, and D in Figure 1-1) are all trunk ports. The user access switches B, C, and D connect to PCs in various departments via access ports, and VLANs correspond to sub VLANs configured on the downlink ports of the core switch, so that access users are in different VLANs to prevent ARP spoofing. The core switch A connects to various servers, such as the authentication server and the DHCP server. Super VLANs and sub VLANs are configured on the downlink ports. One super VLAN correspond to multiple sub VLANs, and each sub VLAN represents an access user.

Deployment

- On the core switch, different access users are identified by VLAN and port numbers. Each access user (or a group of access users) corresponds to one VLAN. The ports on each access switch that connect to downstream users are configured as access ports, and one user VLAN is assigned to each access user according to VLAN planning. The core switch does not forward ARP requests. The core switch replies to the ARP requests from authenticated users only, so as to prevent ARP spoofing. On the core switch A, user VLANs are regarded as sub VLANs, super VLANs are configured, and SVIs corresponding to the super VLANs are configured as user gateways.

- On the downlink ports of the core switch (switch A in this example) that connect to the teachers' living area and the students' living area, both dot1x authentication and Web authentication are enabled, so that users can freely select either authentication mode for Internet access.
- Any special department (such as the headmaster's office in this example) can be allocated to a particular VLAN, and this VLAN can be configured as an authentication-exemption VLAN so that users in this department can access the Internet without authentication.

1.3 Basic Concepts

IPv4 User Capacity

To ensure network stability for online users and stable device running, you can limit the number of IPv4 access users.

The number of IPv4 access users is not limited by default. Authenticated users are allowed to go online until the number of online users reaches the maximum capacity allowed by the hardware.

IPv4 access users include 802.1X authentication users such as authorized IP users, web authentication users, and IP users with static IP-MAC bindings, including IP Source Guard and ARP Check bindings.

User Online-Status Detection

For a chargeable user, accounting starts immediately after the user passes the authentication and gets online. The accounting process does not end until the user actively gets offline. Some users, however, forget to get offline when leaving their PCs, or cannot get offline because of terminal problems. Then the users suffer certain economical losses as the accounting process continues. To more precisely determine whether a user is really online, we can preset a traffic value, so that the user is considered as not accessing the Internet and therefore directly brought offline when the user's traffic is lower than the preset value in a period of time or there is not traffic of the user at all in a period of time.

Features

Feature	Function
User Online-Status Detection	You can specify whether to detect the traffic of online users, so that a user is forced offline when the traffic of the user is lower than a preset value in a period of time.
User Policy Rules	After a user is successfully authenticated, the server may push some control policy names on this user. In this case, these control policy names need to be parsed by the SCC, which will convert these policy names to corresponding policy rules, and install the policies.

1.3.1 User Online-Status Detection

After a user accesses the Internet, the user may forget to get offline or cannot actively get offline due to terminal faults. In this case, the user will keep being charged and therefore will suffer a certain economical loss. To protect the benefits of users on the Internet, the device provides a function to detect whether the users are really online. If the device considers that a user is not online, the device actively disconnects the user.

Working Principle

A specific detection interval is preset on the device. If a user's traffic is lower than a certain value in this interval, the device considers that the user is not using the network and therefore directly disconnects the user.

The user online-status detection function applies to only users who get online through dot1x or Web authentication.

1.3.2 User Policy Rules

After a user is successfully authenticated, the server may push some control policy names on this user. In this case, these control policy names need to be parsed by the SCC, which will convert these policy names to corresponding policy rules, and install the policies.

Working Principle

You can configure on a device the corresponding policy names, under which a speed-limit policy and filtering policy can be configured. After the user passes the authentication and the name of this policy is configured, corresponding speed-limit policy and filtering policy will take effect.

The filtering policy can be applied to user groups to control the use of user group-based policy.

- One filtering policy can be associated with only one ACL.
- The filtering policy cannot be deleted or modified after being applied to the user group.
- The policy needs to be configured only for users that go online through dot1x authentication or Web authentication.

1.4 Configuration

Configuration Item	Suggestions and Related Commands	
Configuring User Online-Status Detection	Optional configuration, which is used to specify whether to enable the user online-status detection function.	
	offline-detect interval threshold	Configures the parameters of the user online-status detection function.
	no offline-detect	Disables the user online-status detection function.
	default offline-detect	Restores the default user online-status detection mode.
Configuring User Policy Rules	(Optional) It is used to specify a user policy rule.	
	[no] rate-policy	Enters speed-limit policy configuration mode.
	upstream average-rate burst-rate	Configures the upstream traffic average and burst threshold.
	no upstream	Deletes the configuration for upstream traffic.

Configuration Item	Suggestions and Related Commands	
	downstream average-rate burst-rate	Configures the downstream traffic average and burst threshold.
	no downstream	Deletes the configuration for downstream traffic.
	[no] filter-policy	Enters filtering policy configuration mode.
	filter_acl	Configures the security ACL associated with the filtering policy.
	no filter_acl	Deletes the security ACL associated with the filtering policy.
	[no] service-policy	Enters user policy configuration mode.
	rate-policy apply	Configures the speed-limit policy to be used.
	no rate-policy	Deletes the speed-limit policy in use.
	filter-policy apply	Configures the filtering policy to be used.
	no filter-policy	Deletes the filtering policy in use.

1.4.1 Configuring User Online-Status Detection

Configuration Effect

After the user online-status detection function is enabled, if a user's traffic is lower than a certain threshold within the specified period of time, the device automatically disconnects the user, so as to avoid the economical loss incurred by constant charging to the user.

Precautions

It should be noted that if disconnecting zero-traffic users is configured, generally software such as 360 Security Guard will run on a user terminal by default. Then such software will send packets time and again, and the device will disconnect the user only when the user's terminal is powered off.

Configuration Method

↘ Configuring User Online-Status Detection

- Optional configuration. A user is disconnected if the user does not involve any traffic within eight hours by default.
- This configuration only works on the configured devices and does not affect other devices in the same network.

Command	**offline-detect interval** *interval* **threshold** *threshold* **no offline-detect** **default offline-detect**
Parameter	*interval*: This parameter indicates the offline-detection interval. The value range is from 1 to 65535

Description	in minutes. The default value is 8 hours, that is, 480 minutes. *threshold*: This parameter indicates the traffic threshold. The value range is from 0 to 4294967294 in bytes. The default value is 0, indicating that the user is disconnected when no traffic of the user is detected. **no offline-detect**: Disables the user online-status detection function. **default offline-detect**: Restores the default value. In other words, an online user will be disconnected when the device detects that the user does not have any traffic within eight hours.
Defaults	8 hours
Command Mode	Global configuration mode
Usage Guide	Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specific threshold within a specific period of time. Use the **no offline-detect** command to disable the user online-status detection function, or use the **default offline-detect** command to restore the default detection mode.

Verification

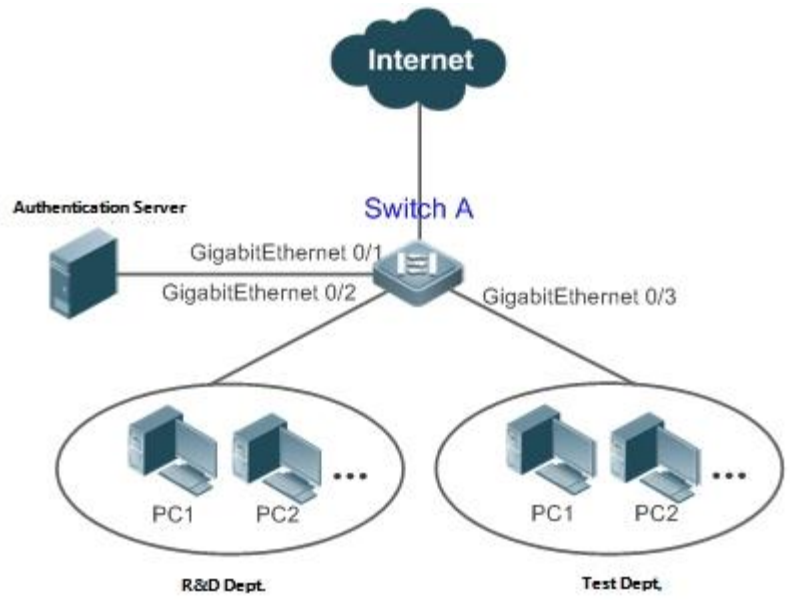
Check the user online-status detection configuration using the following method:

- After the user online-status detection function is enabled, power off the specified authenticated terminal after the corresponding user gets online. Then wait for the specified period of time, and run the online user query command associated with dot1x or Web authentication on the device to confirm that the user is already offline.

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring User Online-Status Detection so that a User Is Disconnected if the User Does Not Have Traffic Within Five Minutes

Scenario **Figure 1-2**	

Configuration Steps	● Enable dot1x authentication on the access port MTGi 0/2, and configure authentication parameters. The authentication is MAC-based. ● Configure user online-status detection so that a user is disconnected if the user does not have traffic within five minutes.
Switch A	sw1(config)# offline-detect interval 5 threshold 0
Verification	● Perform dot1x authentication using dot1x SU client for a PC in the R&D department, so that the PC gets online. Then power off the PC, wait for 6 minutes, and run the online user query command available with dot1x authentication on switch 1 to confirm that the user of the PC is already offline.
Switch A	sw1(config)#show running-config | include offline-detect offline-detect interval 5

1.4.2 Configuring User Policy Rules

Configuration Effect

After user policy rules are configured, you can perform speed-limit configuration for an authenticated user of specified policy names based on these policy rules.

Notes

An authentication server is required to push corresponding policy attributes. Existing policy rules support speed limit configuration and filtering configuration of wireless platforms.

Configuration Steps

↘ Configuring User Policy Rules

- Optional.
- Configure the speed-limit policy and filtering policy first. Then configure the speed-limit policy name in the user policy rule.
- One filtering policy can be associated with only one security ACL.

The burst thresholds of upstream and downstream parameters must not be smaller than the average.

Command	**rate-policy** *name* **{downstream | upstream } average-rate** *avg-threshold* **burst-rate** *burst-threshold*
Parameter Description	***name***: Indicates the name of a speed-limit policy. ***avg-threshold***: Indicates the traffic average, in the unit of KBps. The value ranges from 8 to 261,120. ***burst-threshold***: Indicates the traffic burst threshold, in the unit of KBps. The value ranges from 8 to 261,120. The burst threshold must not be smaller than the average.

Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Speed-limit strategy rules must be configured first.

Command	**filter-policy** *name* **filter-acl** { *acl-name* | *acl-id* }
Parameter Description	*name*: Indicates the name of a filtering policy. *acl-name*: Indicates the name of the security ACL associated with the filtering policy. *acl-id*: Indicates the ID of the security ACL associated with the filtering policy.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Filtering strategy rules must be configured first.

Command	**service-policy** *service-name* **rate-policy** *rate-name* **apply** **filter-policy** *filter-name* **apply**
Parameter Description	***service-name***: Indicates the name of a user policy. ***rate-name***: Indicates the name of the speed-limit policy to be used. *filter-name*: Indicates the name of the filtering policy to be used.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A speed-limit policy and filtering policy can be used user policy rules only after they are configured.

Verification

You can check the configuration effect of a policy rule as follows:

- After a speed-limit policy is configured and the user goes online through authentication, check the speed-limit policy entry corresponding to the WQoS.
- After a filtering policy is configured and the user goes online through authentication, check the ACL entry corresponding to the ACLK.
- Run **show running** to check the user policy configuration.

Configuration Example

↘ Specifying the Speed-limit Policy of an Authenticated User Using a User Policy Rule

Configuration Steps	● Enable Web control on WLAN 1 and configure the corresponding user policy name on a server. ● Configure a user policy rule and specify a speed-limit policy.

AP 1	Hostname(config)# rate-policy user-rate Hostname(config-rate-policy)#upstream average-rate 10 burst-rate 10 Hostname(config-rate-policy)#downstream average-rate 10 burst-rate 10 Hostname(config)# ip access-list extended user_2000 Hostname(config)# filter-policy user-filter Hostname(config-filter-policy)#filter-acl user_2000AC(config)# service-policy user-policy Hostname(config-service-policy)# rate-policy user-rate apply Hostname(config-service-policy)# filter-policy user-filter apply
Verification	● After the user passes authentication, display upstream and downstream packets speeds.

↘ Configuring an ACL and Associating it with a Specified Filtering Policy

Configuration Steps	● Configure an ACL and associate it with a specified filtering policy.
	Hostname(config)# ip access-list extended user_2000 Hostname(config)# filter-policy user-filter Hostname(config-filter-policy)#filter-acl user_2000
Verification	● Run **show running** to check the user group policy configuration.

1.5 Monitoring

Displaying

N/A

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, close the debugging switch immediately after use.

Description	Command
Debugs the SCC running process.	**debug scc event**
Debugs SCC user entries.	**debug scc user** [**mac** | **author** | **mac**]
Debugs ACLs stored in the current SCC and delivered by various services.	**debug scc acl-show summary**
Debugs all ALCs stored in the current SCC.	**debug scc acl-show all**

Configuring Wireless QoS

1. Configuring WLAN QoS
2. Configuring WMM

1 Configuring WLAN QoS

1.1 Overview

WLAN QoS (WQoS) is a wireless bandwidth control technology. It involves rate limiting and fair scheduling,.

Rate limiting is used to limit the traffic of access points (APs), WLAN, or STAs, thus preventing the traffic from exceeding a specified range. Rate limiting is applicable to scenarios where some STAs occupy too much bandwidth and other STAs do not have sufficient bandwidth.

Fair scheduling, by dividing the time equally, resolves the problem that some nodes occupy the air interfaces for a longer time, particularly low-rate nodes. Fair scheduling is applicable to all wireless networks.

An authorized STA that is connected to a wireless network may be used as a proxy server by other STAs. As a result, unauthorized STAs connect to the wireless network without permissions. Intranet proxy prevention is used to address this issue. Intranet proxy prevention is suitable for scenarios where unauthorized proxy servers must be eliminated from the intranet.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society
- Wi-Fi: WMM Specification version 1.1

1.2 Applications

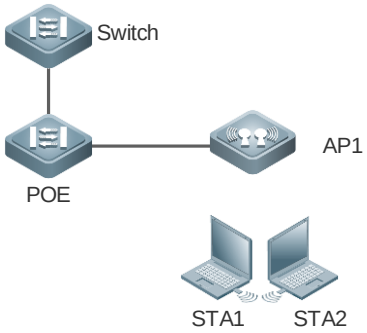
Application	Description
Bandwidth Limiting in Fat AP Networking	The bandwidth is limited in fat AP networking.

1.2.1 Bandwidth Limiting in Fat AP Networking

Scenario

On a wireless network, a fat AP is deployed. The AP is configured with rate limiting for the WLAN and STAs, and is enabled with fair scheduling and intranet proxy prevention.

Figure 1-1



Deployment

Enable WQoS on the AP.

1.3 Features

Basic Concepts

Rate Limiting

To better utilize the limited network resources and serve more users efficiently, the access device need to support rate limiting. When the traffic rate conforms to the committed rates, packets are allowed to pass; otherwise, packets are discarded.

The following parameters are used to evaluate the traffic:

- Average Data Rate: it is the average flow rate that is allowed. It is also called committed information rate (CIR).
- Burst Data Rate: it is the maximum acceptable rate of each burst data, also called committed burst size (CBS).The configured CBS must be greater than the maximum packet length, that is, the maximum rate at which data is sent in a period of 10 milliseconds. (The CBS in the unit of kbps is equal to the maximum traffic in a period divided by 10 milliseconds).

Fair Scheduling

Fair scheduling allows STAs in the same frequency band of the same AP to share the wireless network resources provided by the AP fairly. The fair scheduling function can prevent low-speed STAs from decreasing the throughput of the entire wireless network, and provide smoother network experience for STAs. Besides, the fair scheduling function provides users with better experience by monitoring changes in the traffic of each STA intelligently and adjusting the proportion of the wireless bandwidth used by each STA dynamically. In software version later than 10.4(1T19)p1, different priorities can be configured for STAs in fair scheduling so that specified users can preferentially enjoy the wireless bandwidth.

Intranet Proxy Prevention

In the software version later than 10.4(1T19)p1, intranet proxy prevention is designed to detect the STA that is used as the proxy server for other STAs on a wireless intranet, achieving accurate monitoring of the STA quantity and network traffic.

Traffic-free Network Segment

In specific networking, traffic of users' access to specific network segments does not need to be counted or billed.

Overview

Feature	Description
Rate Limiting	Limits the rates of an AP, a WLAN, or a STA to that the rate does not exceed the limit.
Fair Scheduling	Associates a STA with other STAs in the same frequency band of the same AP to share the wireless network resources provided by the AP, thus sharing the bandwidth of the wireless network in a fair manner.
Intranet Proxy Prevention	Detects the STA that is used as the proxy server for other STAs on a wireless intranet, achieving accurate monitoring of the STA quantity and network traffic.
Traffic-free Network Segment	Addresses the issue that traffic of users' access to specific network segments does not need to be counted or billed. Customers expect to control users' access to specific network segments, for example, access to internal websites and designated servers. The access traffic is not billed.
Dynamic Rate Limiting	Dynamically adjust STA rate limit based on channel utilization.

1.3.1 Rate Limiting

Rate limiting is used to limit the rates of an AP, a WLAN, or a STA to ensure that the rate does not exceed a certain range.

Working Principle

Rate limiting is implemented based on the token bucket.

- The token bucket records the number of bytes that can pass in a certain period of time.
- In each period, the number of data bytes that can pass is calculated based on the configured CIR and CBS, thereby adjusting the size of the token bucket.
- When a packet arrives at the device, the device determines the number of bytes of the packet against the token bucket size. When the number of bytes of the packet is smaller than the token bucket size, the packet is allowed to pass and the token bucket is reduced. When the number of bytes of the packet is larger than the token bucket size, there are two ways to process the packet: traffic shaping and traffic policing. Traffic shaping caches the packet and continues to send the packet until the permit notification of the token bucket is sent. Traffic policing directly discards the packet. The traffic shaping algorithm makes traffic smooth and less volatile; the traffic policing algorithm makes traffic more volatile.
- On an AP, traffic shaping is used to implement rate limiting of an AP, a STA, or a WLAN.

1.3.2 Fair Scheduling

Fair scheduling, by dividing the time equally, resolves the problem that some nodes occupy the air interfaces for a longer time, particularly low-rate nodes.

Working Principle

Owing to the special characteristics of the wireless network, STAs (including APs) on the same network share the air interface resources, which is also a bottleneck of STA performance. This is one of the differences between the wired and wireless networks. Traditional packet scheduling often adopts the first in first out (FIFO) mode. On one wireless network, every STA that needs to transmit data want to occupy the air interface resources whenever possible. Transmission of overwhelming low-rate packets results in long-time occupation of the air interfaces. Thereby, the lasting queue take-up causes packet loss and degrades the overall performance of the network.

In the real wireless scenarios, STAs often differ in types and performance. Consequently, some STAs always cannot obtain the resources, or get super slow response. What is worse, these STAs cannot access the network, which seriously affects user experience.

To settle the problems, it is essential to ensure that each STA is able to obtain resources on air interfaces fairly. That is, every STA that needs to transmit data can occupy the air interfaces for a fair period of time. Fair scheduling of the wireless links can be achieved by ways as follows: Predict the traffic of every STA based on the STA-specific information (such as negotiated rates and aggregation types) and the valid bytes of packets, convert the traffic to the number of packets that can be transmitted by every STA, and adjust the allowed packet number to allocate the bandwidth to every STA over the air interfaces and implement traffic shaping. With fair scheduling, each STA occupies the air interfaces for an equal period of time, which effectively avoids poor performance of some STAs and thus improves user experience.

1.3.3 Intranet Proxy Prevention

An authorized STA that is connected to a wireless network may be used as a proxy server by other STAs. As a result, unauthorized STAs connect to the wireless network without permissions. Intranet proxy prevention is used to address this issue.

Working Principle

Internet proxy prevention is mainly used to determine whether a packet from a STA meets requirements of a proxy server. If not, the STA is contained. The AP supports the TTL detection policy and TCP source port detection policy:

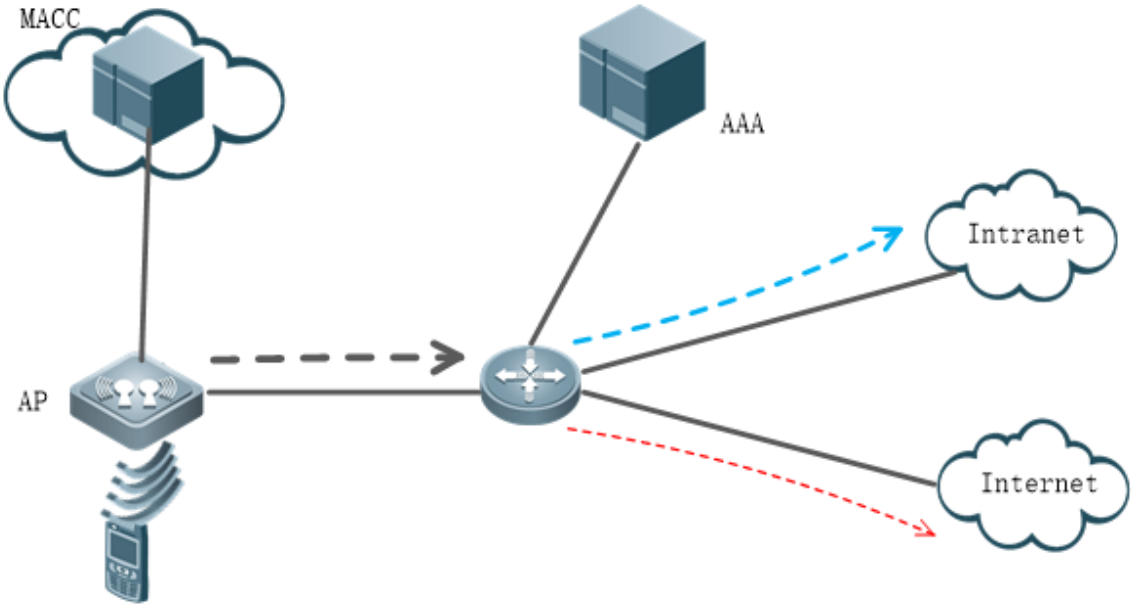
- TTL detection policy: detects whether the TTL in an IP packet sent by a STA to the AP is within the proper range. If the TTL is out of the range, the STA is a proxy server.
- TCP source port detection policy: detects whether the number of ports used in TCP packets from a STA is within the proper range. If the value is out of the range, the STA is a proxy server.

1.3.4 Traffic-free Network Segment

This function addresses the issue that traffic of users' access to specific network segments does not need to be counted or billed. Customers expect to control users' access to specific network segments, for example, access to internal websites and designated servers. The access traffic is not billed.

Working Principle

Figure 1-2



In the preceding topology, MACC manages the AP, and a STA is associated with the AP and accesses the network to generate traffic. The black dashed line indicates the total traffic generated by the STA, the green dashed line indicates the intranet access traffic, and the red dashed line indicates the extranet access traffic. When the user accesses the intranet, the user is not billed (traffic is not counted). When the user accesses the extranet, the user needs to be billed (traffic is counted). The RADIUS server bills users by the traffic reported by WQoS, which includes the total traffic and pass-through traffic. The traffic used for billing is the total traffic minus the pass-through traffic.

When a traffic-free IP segment is configured, the IP segment can be added to the WQoS pass-through IP list. When WQoS calculates traffic, the traffic of access to the specified network segment is considered as pass-through traffic. Then the pass-through traffic is subtracted when the RADIUS server counts traffic for billing. In this case, the traffic of access to the specified network segment is not billed.

1.3.5 Dynamic Rate Limiting

Dynamic rate limiting, as compared to traditional rate limiting, only requires configuration of a switch, and no bandwidth limits need to be specified for individual STAs. With traditional rate limiting, STAs cannot be rate-limited in a multi-STA scenario when rate limits are high, while air interface resources cannot be properly utilized at idle time when rate limits are low. In contrast, dynamic rate limiting allows you to apply stricter rate limiting to the STAs when multiple users preempt air interfaces and apply loose rate limiting to the STAs when

the air interfaces are comparatively idle. In this way, air interfaces resources can be properly allocated while network experience of users is ensured.

1.4 Configuration

Configuration	Description and Command	
Configuring Rate Limiting	(Mandatory) It is used to enable rate limiting.	
	wlan-qos ap-based	Configures AP-based rate limiting on an AP.
	wlan-qos netuser	Configures STA-based rate limiting on an AP.
	wlan-qos wlan-based	Configures WLAN-based rate limiting on an AP.
Configuring Fair Scheduling	(Mandatory) It is used to enable fair scheduling.	
	fair-schedule	Enables fair scheduling.
	(Optional) It is used to adjust the STA priority during fair scheduling.	
	sta-fair	Configures the fair scheduling priority of a STA.
Configuring Intranet Proxy Prevention	(Mandatory) It is used to configure an intranet proxy prevention policy and enable intranet proxy prevention detection.	
	illegal-sta-check ip ttl	**illegal-sta-check ip ttl**
	illegal-sta-check tcp source-ports	**illegal-sta-check tcp source-ports**
Configuring Dynamic Rate Limiting	(Optional) It is used to configure dynamic rate limiting.	
	smart-rate-control enable	Configures dynamic rate limiting.
	smart-rate-control config low-rate-sta	Configures associated rate threshold for low-speed STAs.
	smart-rate-control config rate-limit-step	Configures rate limiting factor.
	smart-rate-control config sampling	Configures timer parameters.
	smart-rate-control config threshold channel-using	Configures channel utilization threshold.
	smart-rate-control config threshold rate-guard	Configures guaranteed bandwidth enforcement.
	smart-rate-control config threshold rate-limit	Configures rate limiting scope.
	smart-rate-control config wlan-loss	Configures wireless loss.

1.4.1 Configuring Rate Limiting

Configuration Effect

- Only the committed resource is allocated to a stream based on the actual situation of the network, which prevents network congestion caused by burst stream.

Notes

- On a fat AP, CLI commands are configured in global configuration mode.
- The following rate limiting modes are applied to STAs: wlan-based per-user-limit, wlan-based per-ap-limit intelligent, ap-based per-user-limit, ap-based total-limit intelligent, and netuser. Only one of the preceding rate limiting mode can take effect on a STA. The five rate limiting modes are listed in descending order of priority: netuser, wlan-based per-ap-limit intelligent, wlan-based per-user-limit, ap-based total-limit intelligent, and ap-based per-user-limit.
- wlan-based total-limit, wlan-based per-ap-limit, ap-based total-limit, and STA rate limiting are applied to different objects, so they can work simultaneously. They are not differentiated by priority.

Configuration Steps

↘ Configuring AP-based Rate Limiting

- Mandatory.
- Configure rate limiting per single user on a fat AP in global configuration mode.

Command	**wlan-qos ap-based** { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* **wlan-qos ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**
Parameter Description	**per-user-limit**: indicates that rate limiting is implemented on every STA on the AP. **total-user-limit**: indicates that rate limiting is implemented on all STAs on the AP. **intelligent**: indicates whether rate limiting is implemented on all STAs on the AP intelligently. **down-streams**: indicates that rate limiting is implemented on the downlink traffic of the AP. **up-streams**: indicates that rate limiting is implemented on the uplink traffic of the AP. *average-data-rate*: indicates CIR. The unit is 8 kbps. The value ranges from 8 to 261,120. *burst-data-rate*: indicates CBS. The unit is 8 kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured. If **total-user-limit** is configured, intelligent rate limiting is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

- Configure rate limiting per device on a fat AP in global configuration mode.

Command	**wlan-qos ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**
Parameter Description	**total-user-limit**: rate-limits the AP. **intelligent**: indicates whether intelligent rate limiting is performed for the total traffic. **down-streams**: configures the downlink rate limit on the AP. **up-streams**: configures the uplink rate limit on the AP.
Defaults	By default, intelligent rate limiting is not enabled.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuring STA-based Rate Limiting

- Mandatory.
- On a fat AP, run the **wlan-qos netuser** command in global configuration mode to configure STA-based rate limiting.

Command	**wlan-qos netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	*mac-address*: indicates the MAC address of a STA. **inbound**: indicates that rate limiting is implemented on the uplink traffic of a STA. **outbound**: indicates that rate limiting is implemented on the downlink traffic of a STA. *average-data-rate*: indicates CIR. The unit is 8 kbps. The value ranges from 8 to 261,120. *burst-data-rate*: indicates CBS. The unit is 8 kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring WLAN-based Rate Limiting

- Mandatory.
- On a fat AP, run the **wlan-qos wlan-based** command in global configuration mode to configure WLAN-based rate limiting.

Command	**wlan-qos wlan-based** { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* **wlan-qos wlan-based** { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams** } **intelligent**
Parameter Description	**per-user-limit**: indicates that rate limiting is implemented on every STA on the WLAN. **total-user-limit**: indicates that rate limiting is implemented on all STAs on the WLAN. **intelligent**: indicates whether rate limiting is implemented on all STAs on the WLAN intelligently. **per-ap-limit**: indicates that AP-based rate limiting is implemented. **down-streams**: indicates that rate limiting is implemented on the downlink traffic of the WLAN. **up-streams**: indicates that rate limiting is implemented on the uplink traffic of the WLAN. *average-data-rate*: indicates CIR. The unit is 8 kbps. The value ranges from 8 to 261,120. *burst-data-rate*: indicates CBS. The unit is 8 kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured.
Command Mode	Global configuration mode
Usage Guide	N/A

- Configure intelligent rate limiting for total traffic on the WLAN on the fat AP.

Command	**wlan-qos wlan-based** { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams** } **intelligent**
Parameter	*wlan-id*: specifies the WLAN ID.

Description	*ssid:* specifies the SSID of the WLAN. **down-streams**: configures rate limiting parameters for downlink traffic of the WLAN. **up-streams**: configures rate limiting parameters for uplink traffic of the WLAN. **intelligent**: indicates whether intelligent rate limiting is performed for total traffic.
Defaults	Rate limiting is not configured.
Command Mode	Global configuration mode
Usage Guide	N/A

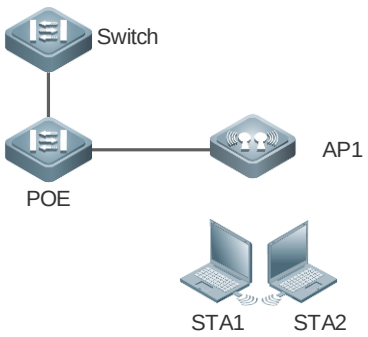
Verification

N/A

Configuration Example

Configuring AP-based Rate Limiting

Scenario Figure 1-3



Configuration Steps	● In global configuration mode, configure rate limiting for per-user downlink traffic on the AP.
AP	Hostname#configure terminal Hostname(config)# wlan-qos ap-based per-user-limit down-streams average-data-rate 800 burst-data-rate 1600 Hostname(config)# exit
Verification	Run the **show dot11 ratelimit ap** command to check the configuration.
AP	Hostname#show dot11 ratelimit ap AP name :Local_AP, ratelimit info(unit :8kbps): Per-user-limit: Upstream : average rate - 0 , burst rate - 0 Downstream: average rate - 800 , burst rate - 1600 Total-user-limit: Upstream : average rate - 0 , burst rate - 0 Downstream: average rate - 0 , burst rate - 0

Common Errors

N/A

1.4.2 Configuring Fair Scheduling

Configuration Effect

- The fair scheduling function can prevent low-speed STAs from decreasing the throughput of the entire wireless network, and provide smoother network experience for STAs.

Notes

- On a fat AP, configure fair scheduling in global configuration mode, and run the **show running-config** command to display the configurations.

Configuration Steps

↘ Enabling Fair Scheduling

- Mandatory.
- On a fat AP, run the **fair-schedule** command in global configuration mode to enable fair scheduling.
- Enabling fair scheduling can allocate time to STAs in a fair manner.

Command	**fair-schedule**
Parameter Description	N/A
Defaults	By default, fair scheduling is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Fair Scheduling Priority

- (Optional) Perform this configuration if you need to change the fair scheduling priority of a STA.
- On a fat AP, run the **sta-fair** command in global configuration mode to configure the fair scheduling priority.

Command	**sta-fair** *mac-address* **priority** *priority*
Parameter Description	*mac-address*: indicates the MAC address of a STA. *priority*: indicates the priority. The value ranges from 1 to 6.
Defaults	By default, the priority is 1 for all STAs. A greater value indicates a higher priority, and a higher priority indicates that a longer time is allocated to the STA.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

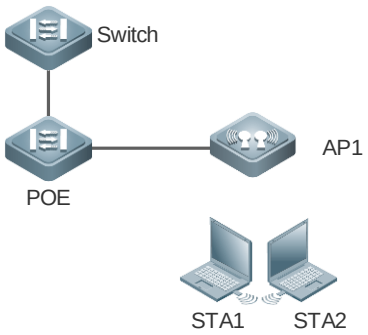
- Run the **show running** command to display the configuration.

Configuration Example

Enabling Fair Scheduling and Setting the Priority

Scenario

Figure 1-4



Configuration Steps	Enable fair scheduling and configure the STA priority.
AP	Hostname#configure terminal Hostname(config)#fair-schedule Hostname(config)# sta-fair 1111.1111.1111 priority 6 Hostname(config)# end
Verification	Run the **show running-config** command to display the configuration.
AP	Hostname# show running ! sta-fair 1111.1111.1111 priority 6 !

Common Errors

N/A

1.4.3 Configuring Intranet Proxy Prevention

Configuration Effect

- Detect the STA that is used as the proxy server for other STAs on a wireless intranet, achieving accurate monitoring of the STA quantity and network traffic.

Notes

N/A

Configuration Steps

Enabling Intranet Proxy Prevention

- Mandatory. You can choose the TTL detection policy or TCP source port detection policy.
- Run the **illegal-sta-check** command to enable intranet proxy prevention.
- Enable intranet proxy prevention to detect the STA that is used as the proxy server for another STA and contain the STA.
- Enable intranet proxy prevention and use the TTL detection policy.

Command	**illegal-sta-check ip ttl**
Parameter Description	N/A
Defaults	By default, intranet proxy prevention is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

- Enable intranet proxy prevention and use the TCP source port detection policy.

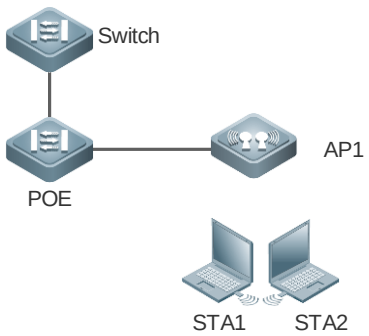
Command	**illegal-sta-check tcp source-ports** [*port-num*]
Parameter Description	*port-num*: specifies the upper limit for the number of ports to be detected. The value range is 1–512.
Defaults	By default, intranet proxy prevention is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

↘ Enabling Intranet Proxy Prevention

Scenario Figure 1-5	
Configuration Steps	● Enable intranet proxy prevention in global configuration mode.
AP	Hostname#configure terminal Hostname(config)# illegal-sta-check ip ttl Hostname(config)# illegal-sta-check tcp source-ports

	Hostname(config)# end
Verification	Run the **showap-config running** command to display the configuration.
AP	Hostname# show running ! illegal-sta-check ip ttl illegal-sta-check tcp source-ports !

Common Errors

N/A

1.4.4 Configuring Dynamic Rate Limiting

Configuration Effect

- Dynamic rate limiting adjusts STA rate limits based on channel utilization, keeping air interface utilization below 70%.

Notes

- During mixed deployment of APs supporting dynamic rate limiting and APs not supporting dynamic rate limiting, the APs supporting dynamic rate limiting will be suppressed.

Configuration Steps

↘ Enabling Dynamic Rate Limiting Function

- Optional.
- On the AP, run the **smart-rate-control enable** command in global configuration mode.

Command	**smart-rate-control enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring Dynamic Rate Limiting Parameters

- Configure associated rate thresholds for low-speed STAs.

Command	**smart-rate-control config low-rate-sta** *rate-num*
Parameter Description	*rate-num*: Indicates the threshold for associated rate of a low-speed STA. The value ranges from 1 to 500,000, in Kbps.
Defaults	The default value is 30,000, which means the associated rate threshold is 30 Mbps.

Command Mode	Global configuration mode
Usage Guide	When the associated rate of an STA is lower than the threshold for low-speed STAs, the STA is considered as a low-speed STA. When adjusting the rate limiting factor using the **smart-rate-control config rate-limit-step** command, the actual adjustment result for low-speed STAs is different from that for non-low-speed STAs. When increasing the rate limiting factor, for non-low-speed STAs, the percentage increase is as configured. For low-speed STAs, the actual increase factor is only 1/3 of the configured rate limiting factor, i.e., 1/3 * rate-num. When reducing the rate limiting factor, for non-low-speed STAs, the percentage reduction is as configured. For low-speed STAs, the actual reduction factor is 3 times the configured factor, i.e., 3 * rate-num.

- Configure the rate limiting factor.

Command	**smart-rate-control config rate-limit-step { increase** *increase-percent* **| reduce** *reduce-percent* **}**
Parameter Description	*increase-percent*: Indicates the percentage increase of the rate limiting factor. The value ranges from 1 to 100. *reduce-percent*: Indicates the percentage reduction of the rate limiting factor. The value ranges from 1 to 100.
Defaults	The value for increasing the rate limiting factor is 20 by default. The value for reducing the rate limiting factor is 20 by default.
Command Mode	Global configuration mode
Usage Guide	N/A

- Configure timer parameters.

Command	**smart-rate-control config sampling** { **period** *cycle-num* | **times** *times-num* }
Parameter Description	*cycle-num*: Configures the interval for timer sampling, in milliseconds. The value ranges from 1,000 to 10,000. *times-num*: Configures the number of data sampling times before triggering rate adjustment. The value ranges from 1 to 100.
Defaults	Default sampling period is 1,000 ms, and the number of data sampling times is 5.
Command Mode	Global configuration mode
Usage Guide	The timer configuration takes effect in the next scheduling period, with a waiting time of 0–period*times.

- Configure the channel utilization threshold.

Command	**smart-rate-control config threshold channel-using** { **busy** *busy-num* | **clean** *clean-num* | **free** *free-num* }
Parameter	*busy-num*: Configures the threshold percentage for busy channel utilization. The value ranges from 1

Description	to 100. *clean-num*: Configures the threshold percentage for clean channel utilization. The value ranges from 1 to 100. *free-num*: Configures the threshold percentage for free channel utilization. The value ranges from 1 to 100.
Defaults	The threshold for busy channel utilization is 70 by default, which is 40 for free channel utilization and 20 for clean channel utilization.
Command Mode	Global configuration mode
Usage Guide	Configured thresholds should ensure that busy threshold > free threshold > clean threshold.

- Configure guaranteed bandwidth enforcement.

Command	**smart-rate-control config threshold rate-guard** *rate-num*
Parameter Description	*rate-num*: Configures the threshold for guaranteed bandwidth, in the unit of 8 Kbps. The value ranges from 8 to 261,120.
Defaults	Not configured by default.
Command Mode	Global configuration mode
Usage Guide	1. After configuration, the original method of calculating guaranteed bandwidth becomes ineffective and is updated to the newly configured bandwidth. 2. Guaranteed Bandwidth = (Negotiated rate of STA * 0.8 (wireless loss) * (1 – WLAN-loss))/Number of STAs WLAN-loss is wireless loss.

- Configure the rate limiting scope.

Command	**smart-rate-control config threshold rate-limit** { **maximum** *max-num* | **minimum** *min-num* }
Parameter Description	*max-num*: Configures the maximum rate limit value, in the unit of 8 Kbps. The value ranges from 8 to 261120. *min-num*: Configures the minimum rate limit value, in the unit of 8 Kbps. The value ranges from 8 to 261120.
Defaults	The maximum rate limit is 25000 by default, and the minimum rate limit is 8 by default.
Command Mode	Global configuration mode
Usage Guide	1. If the rate limit value is greater than the maximum, the maximum rate limit is canceled. 2. Rate limit value must not be smaller than the minimum.

- Configure the wireless loss.

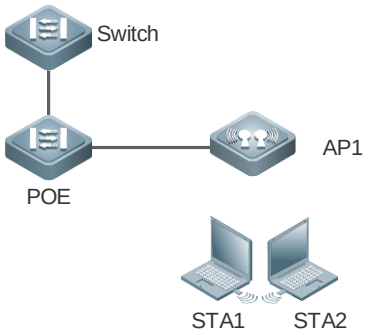
Command	**smart-rate-control config wlan-loss** *loss-num*
Parameter Description	*busy-num*: Configures the percentage of wireless loss. The value ranges from 1 to 100.
Defaults	The wireless loss is 20% by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to check if the dynamic rate limiting feature is enabled and its parameters. By default, this information is not displayed in the configuration.

Configuration Example

Configuring Dynamic Rate Limiting

Scenario **Figure 1-6**	
Configuration Steps	1. Enable dynamic rate control on AP1. 2. Configure the low rate for associated low-speed STAs as 1,024. 3. Set the rate limiting factor to 20%. 4. Configure the timer effective period as 2,000 ms. 5. Set the threshold percentage for busy channel utilization as 80%. 6. Configure the guaranteed bandwidth as 100, equivalent to 800 Kbps (100 * 8 Kbps). 7. Set the minimum rate limiting as 20, equivalent to 160 Kbps (20 * 8 Kbps). 8. Set the wireless loss as 50%.
	Hostname#configure terminal Hostname(config)#smart-rate-control enable Hostname(config)#smart-rate-control config low-rate-sta 1024 Hostname(config)#smart-rate-control config rate-limit-step increase 20

	Hostname(config)#smart-rate-control config sampling period 2000 Hostname(config)#smart-rate-control config threshold channel-using 80 Hostname(config)#smart-rate-control config threshold rate-guard 100 Hostname(config)#smart-rate-control config threshold rate-limit 20 Hostname(config)#smart-rate-control config wlan-loss 50
Verification	Run the **show running-config** command to display the configuration.
	Hostname# show running-config smart-rate-control enable smart-rate-control config low-rate-sta 1024 smart-rate-control config rate-limit-step increase 20 smart-rate-control config sampling period 2000 smart-rate-control config threshold channel-using 80 smart-rate-control config threshold rate-guard 100 smart-rate-control config threshold rate-limit 20 smart-rate-control config wlan-loss 50

Common Errors

- N/A

1.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays WQoS rate limiting information.	**show dot11 ratelimit** { **wlan** | **ap** | **user** }
Displays the latest five rate-limiting records.	**show wqos control rate-limit smart-rc** mac

Debugging

N/A

1 Configuring WMM

1.1 Overview

WMM is a wireless QoS protocol, and this protocol is a subset of the 802.11e protocol.

WMM is used to ensure that high-priority packets are preferentially sent, thereby assuring the quality of the voice and video applications in a wireless network.

This document consists of two parts, that is, WMM service and QoS packet priority mapping.

- WMM service: The WMM service is used to differentiate the capabilities of the access channels with different priorities, thereby ensuring that channel resources are allocated based on data flow priorities. Users can adjust the values of the EDCA parameters for the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.
- QoS packet priority mapping: Wireless-to-wired QoS mapping and wired-to-wireless QoS mapping help to implement end-to-end QoS in the entire network, thereby assuring the quality of high-priority service flows.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society

1.2 Applications

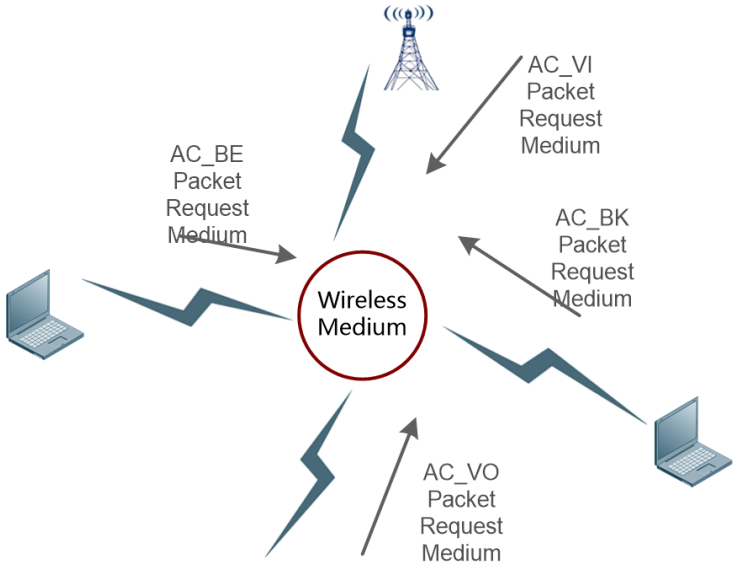
Application	Scenario
WMM Service	Competition process of channels with different priorities.

1.2.1 WMM Service

↘ Scenario

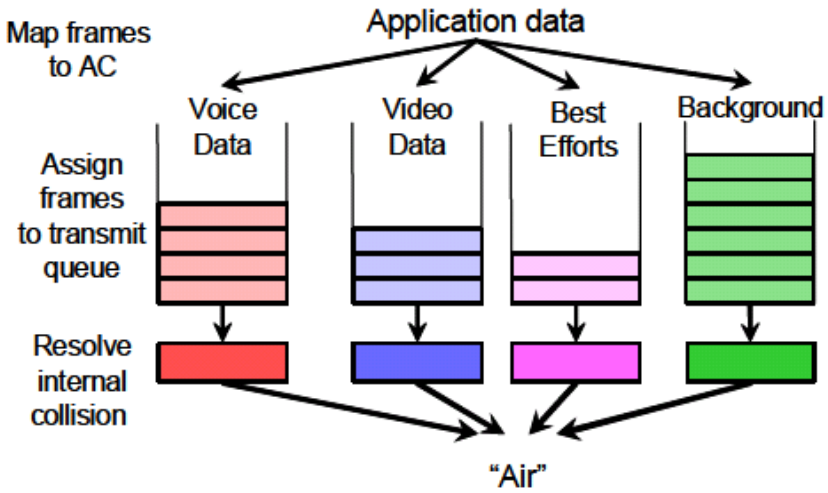
The medium for wireless communication is radio. In a specified frequency band, channels are shared during wireless network communication. In the same RF environment, the uplink and downlink traffic of different sites conflicts. Therefore, the problem how communication participants compete for shared channels needs to be solved to ensure wireless QoS. As shown in Figure 3-1, there are packets of four different priorities in the same wireless network environment (the packets from high priority to low are as follows: AC_VO > AC_VI > AC_BE > AC_BK). When multiple supplicants request the medium to send packets and compete for channels, the competition and coordination mechanism is enabled to determine which supplicant's packet can access the medium. The higher the packet’s priority is, the more likely the packet is to access the channel.

Figure 1-1 Channel competition



In a wireless network, since the medium is special, packet damage caused by packet loss and signal interference occurring during transmission over the network is quite serious. Different wireless transmission parameters of the mechanism need to be retransmitted to ensure arrival of packets. However, it is unpractical that preferable parameters are adopted for all packets. In this case, to provide services having high reliability and timeliness requirements, you can classify packets. In short, provide network services of different quality based on various requirements. That is, process key data packets having high timeliness requirement preferentially, and assign a low processing priority to general packets not having high timeliness requirement. To make a network carry different services, you must ensure that the network not only provides single service with the best QoS, but also provides different service with different QoS. Therefore, the QoS of a wireless AP requires the classification/identification of packets for identifying different data flows and providing service of different quality.

Figure 1-2 Wireless QoS multi-priority queue



Deployment

The device should be configured with the following key points:

- Enable the WMM.
- Set WMM EDCA competition parameters. Generally, default values are adopted.

1.3 Features

Basic Concepts

Access Class

According to the WMM standard, access data flows have four priorities. Each priority can be regarded as a class. From the lowest priority to the highest priority, the sequence is as follows: AC_BK, Background < AC_BE, Best Efforts < AC_VI, Video Data < AC_VO, Voice Data.

EDCA Competitive Mechanism

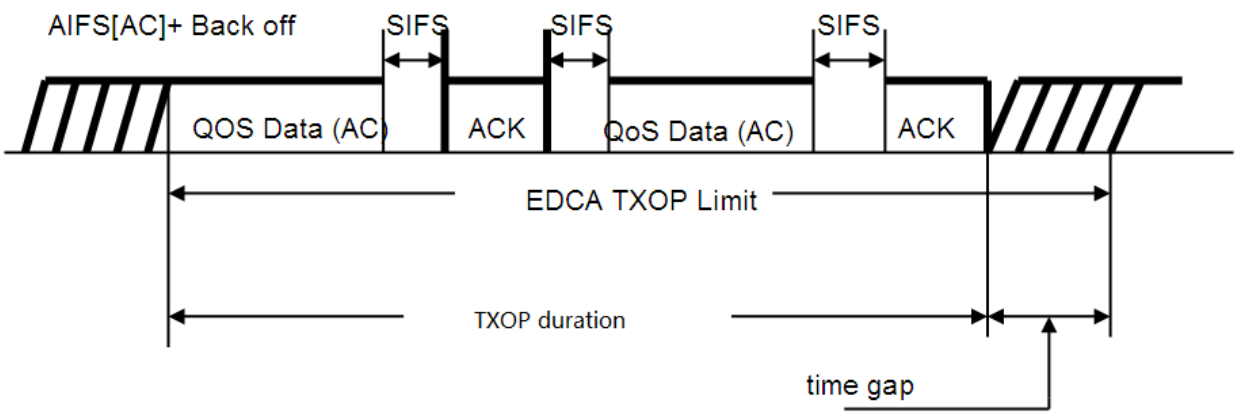
The EDCA competitive mechanism is the core of the IEEE 802.11e. The EDCA differentiates the access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities. Enhanced distributed channel access (EDCA) not only retains distributed channel competition between the AP and STA, but also introduces internal competition of four internal priority classes of QAP/QSTA. In this way, EDCA introduces the channel competition mechanism for differentiating the priority classes between different QAPs and QSTAs through the wireless air interface. Competition for channels is implemented by configuring EDCA competition parameters of different priority classes. The QAP pushes the configuration to the QSTA and controls the access capability of the QSTA. Competition parameters include AIFS, TXOP Limit, CWmin, and CWmax.

EDCA Parameters

The EDCA competition parameters are listed as follows:

- AIFSN (Arbitration Inter Frame Spacing Number): In the 802.11 protocol, the Distributed Inter-frame Spacing (DIFS) is a fixed value. However, the DIFS for different ACs of the WMM can be set to different values. A larger AIFSN value means a longer DIFS. A shorter DIFS means a bigger probability of preempting channels.
- ECWmin (Exponent form of CWmin) and ECWmax (Exponent form of CWmax) determine the average backoff time. Larger ECWmin and ECWmax mean a longer backoff time.
- TXOP (Transmission Opportunity): maximum duration for preempting channels after successful competition by a user at one time. A larger TXOP means a longer duration for a user to preempt channels. If the TXOP value is 0, only one packet is sent after channel preemption each time. If a frame is too large to be completely sent within the TXOP, this frame must be segmented.

Figure 1-3 TXOP successive frame transmission



ACK Policy

Two ACK policies are available, that is, Normal ACK and No ACK.

- Normal ACK: After receiving a unicast packet successfully, the recipient returns an ACK response.
- No ACK: In the environment with high communication quality and little interference, you can configure the mechanism of not returning an ACK packet for the flow of a certain priority for confirmation, saving the channel resource. During wireless packet interaction, it is not necessary that an ACK packet is used for confirmation. The No ACK policy helps to improve the transmission efficiency effectively. However, it may cause packet loss.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

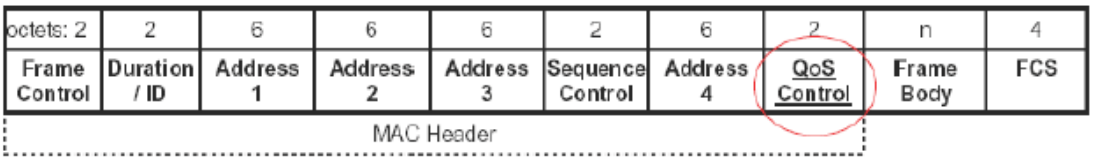
AC Queue Depth

If the queue depth of packets of a certain priority is greater than the preset AC queue depth, subsequent packets are discarded. Otherwise, subsequent packets are added to the queue for processing according to normal logics.

802.11e Priority

802.11e extends the MAC header of 802.11, with the QoS Control domain added, as shown in Figure 3-4.

Figure 1-4 802.11e MAC Header



The QoS Control domain has two bytes. Among them, the first three bits are the TID field, indicating the data form identification code. TID values 0-7 are used for QoS with priorities, indicating the priorities (UP) of users; TID values 8-15 are used for parameter-based QoS, indicating the data flow ID (TSID).

The WMM maps UP to corresponding AC. The following table lists the mapping between the 802.11e priority and AC.

Priority	UP (User Priority)	AC (Access Category)
Lowest	1	Back-ground
	2	Back-ground
	0	Best-effort
	3	Best-effort
	4	Video
	5	Video
	6	Voice
Highest	7	Voice

Priority Mapping Table

After a packet enters a device, the device judges the packet trust mode of the current interface, that is, judges which part of priority information in the received packet is valid. In addition, the device judges the work mode (fat

AP) of the current AP. Then, the device selects a mapping table based on the preset information to perform the priority mapping operation.

Overview

Feature	Description
WMM Service	Configures WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.
QoS Packet Priority Mapping	Configures QoS packet priority mapping, including the QoS packet priority mapping table and priority mapping policy.

1.3.1 WMM Service

Configure WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.

Working Principle

Provide network services of different quality based on various requirements. That is, provide high-quality services for key data packets having high timeliness requirement and process them preferentially, and assign a low processing priority to common packets not having high timeliness requirement. According to the WMM standard, access data flows have four priorities. Each priority can be regarded as a class. The EDCA differentiates the access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities.

↘ Enabling WMM

Enable/disable the WMM service. When the WMM service is enabled, the four-level priority queue is used for reception and mapping. When the WMM service is disabled, the default priority queue is used for reception and mapping.

↘ EDCA Competitive Mechanism, AC Queue Depth, and NO ACK Policy

- EDCA competitive mechanism:

EDCA parameters differentiate the channel access capabilities of different priorities. Each AC has its own EDCA channel competition parameters. Users can adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel. The channel competition should be completed automatically by the hardware. The hardware would be engaged in the channel competition after parameters such as CWmin, CWmax, AIFSN, TXOP of each hardware queue are set on the software.

During actual configuration, you can choose to configure the EDCA parameters on the client side or AP side based on application requirements. The configuration of edca-client mainly affects the wmm competition parameters of STA, and the configuration of edca-radio mainly affects the wmm competition parameters of AP.

The QSTA configuration is managed and pushed by the QAP in a centralized manner. The channel competition parameters of QAP and QSTA are mutually independent. Generally, the channel competition parameters of QAP would be slightly increased to ensure competent channel control capability for QAP. QAP would notify the EDCA parameter setting of QAP through the EDCA Parameter Set IE of the frame of beacon or Probe Response, and

push the negotiated EDCA configuration to QSTA through EDCA Parameter Set IE of the (Re) Association Response frame.

- AC queue depth:

Set the AC queue depth. If the queue depth of packets of a certain priority is greater than the preset AC queue depth, subsequent packets are discarded. Otherwise, subsequent packets are added to the queue for processing according to normal logics.

- NO ACK policy:

Enable/disable the NO ACK (No Acknowledgement) policy. The NO ACK policy should be supported by the recipient and the sender at the same time. When the NO ACK policy frame transmission chip does not support NO ACK policy for a queue, the NO ACK policy should be set in the DMA descriptor of each frame sent at each frame sent.

The NO ACK policy is used as an alternative for the method of receiving confirmation (during wireless packet exchange) by using ACK packets in the environment with high communication quality and little interference. The NO ACK policy helps to effectively improve the transmission efficiency. However, if ACK packet for confirmation is not used and the communication quality is poor, the sender would not retransmit the packets even if the recipient has not received the packets, resulting in increasing packet loss rate.

1.3.2 QoS Packet Priority Mapping

Configure QoS packet priority mapping, including the QoS packet priority mapping table and priority mapping policy.

Working Principle

The priority mapping tables provided by the device correspond to relevant priority mapping respectively. Then, a mapping table is selected based on the preset information to perform the priority mapping operation, thereby implementing end-to-end QoS for the entire network.

↘ Packet Priority Mapping

In the IP network, IPv4 packets carry QoS priority tags in three modes, that is, Layer 2-based CoS field (IEEE802.1p) priority, IP layer-based IP priority field ToS priority, and IP layer-based DSCP (Differentiated Services Codepoint) field priority.

For the three QoS priority tags of wired packets, it is sufficient to support the two kinds of QoS (DSCP and dot1P) because DSCP is compatible with ToS. In addition to the preceding three modes, the QoS priority tag mode of dot11e is also available for wireless packets.

As for the determination and execution of packet priority mapping, the device judges the packet trust mode or tag policy of the current interface, that is, judges which part of priority information in the received packet is valid. In addition, the device judges the work mode (centralized forwarding or local forwarding) of the current AP. Then, the device selects a mapping table based on the preset information to perform the priority mapping operation.

1.4 Configuration

Configuration	Description and Command

Configuration	Description and Command	
Configuring the WMM Service	⚠ (Mandatory). It is used to enable the WMM service.	
	wmm enable	Enables the WMM service.
	⚠ (Optional). It is used to configure competition parameters.	
	wmm edca-client	Configures the EDCA parameters for the client.
	wmm edca-radio	Configures the EDCA parameters for the AP.
Configuring the QoS Packet Priority Mapping	⚠ (Optional). It is used to configure the priority mapping. Mapping command for non-interworking versions.	
	wlan-qos map-table	Configures packet priority mapping of the current WLAN.
	⚠ (Optional). It is used to configure the 802.11p QoS mapping policy mechanism. Mapping command for interworking versions.	
	wmm dot1p enable	Enables 802.11p QoS mapping policy mechanism.
	wmm dot1p policy 1q	Configures how to apply the 802.11p QoS mapping policy mechanism for the AP.
	wmm dot1p tag	Configures 802.1p priority.
	⚠ (Optional) . It is used to configure the DSCP QoS mapping policy mechanism. Mapping command for interworking versions.	
	wmm dscp enable	Enables DSCP QoS mapping policy mechanism.
	wmm dscp policy outer-tunnel inner-tunnel	Configures how to apply the DSCP QoS mapping policy mechanism for the AP.
	wmm dscp tag	Configures DSCP identifications.

1.4.1 Configuring the WMM Service

Configuration Effect

- Configure the EDCA competition parameters for the client.
- Configure the EDCA competition parameters for the AP.
- Configure the ACK policy.
- Configure the length of the priority queue.

Notes

- The parameter configuration takes effect after the WMM service is enabled.

- When the WMM service is enabled and the BE queue adopts the default configuration, the Xspeed function dynamically adjusts the parameters of the BE queue.

Configuration Steps

Enabling the WMM Service

- Mandatory.
- Run the **wmm enable** command in interface configuration mode to enable the WMM for the fat AP.
- When the WMM service is enabled, the four-level priority queue is used for reception and mapping. When the WMM service is disabled, the default priority queue is used for reception and mapping.

Command	**wmm enable**
Parameter Description	N/A
Defaults	WMM is enabled by default
Command Mode	Dot11radio interface configuration mode.
Usage Guide	When the WMM service is disabled, the default priority queue is used for reception and mapping.

Configuring the EDCA Parameters for the Client

- Optional configuration.
- By default, the EDCA parameters on the client side are as follows:

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4	94
voice	2	2	3	47

- After the EDCA parameters on the client side and AC queue depth are set, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Command	**wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } [{ **aifsn** *aifsn-value* **cwmin** *cwmin-value* **cwmax** *cwmax-value* **txop** *txop-value* } | **length** *queue-length*]
Parameter Description	**back-ground**: indicates the back-ground queue. **best-effort**: indicates the best-effort queue. **video**: indicates the video queue. **voice**: indicates the voice queue. **aifsn** *aifsn-value*: indicates the aifsn value. Value range: 1-15. **cwmin** *cwmin-value*: indicates the cwmin value. Value range: 0-15. **cwmax** *cwmax-value*: indicates the cwmax value. Value range: 0-15. **txop** *txop-value*: indicates the txop value. Value range: 0-255, unit: 32 μs. **length** *queue-length*: indicates the AC queue length. Value range: 1-255. The default is 255.
Command Mode	Dot11radio interface configuration mode.

Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a configuration error message is displayed.

Configuring the EDCA Parameters for the AP

- Optional.
- By default, the EDCA parameters on the AP side are as follows:

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

- After the EDCA parameters on the AP side and NO ACK policy are set to non-default settings, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.
- Smaller AIFS of a high-priority AC means earlier backoff process. Smaller CWmin and CWmax values mean shorter backoff time. TXOP limit allows an AC to transmit multi-frame packets on it continuously within the SIFS interval after preempting a transmission opportunity. A larger TXOP limit means a lower packet conflict rate and a lower waste of air interface resources.

Command	**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } [{ **aifsn** *aifsn-value* **cwmin** *cwmin-value* **cwmax** *cwmax-value* **txop** *txop-value* } | **noack**]
Parameter Description	**back-ground**: indicates the back-ground queue. **best-effort**: indicates the best-effort queue. **video**: indicates the video queue. **voice**: indicates the voice queue. **aifsn** *aifsn-value*: indicates the aifsn value. Value range: 1-15. **cwmin** *cwmin-value*: indicates the cwmin value. Value range: 0-15. **cwmax** *cwmax-value*: indicates the cwmax value. Value range: 0-15. **txop** *txop-value*: indicates the txop value. Value range: 0-255, unit: 32 μs. **noack**: indicates that the no ack policy is enabled. The no ack policy is disabled by default.
Command Mode	Dot11radio interface configuration mode.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a configuration error message is displayed.

Verification

- You can run the **show running** command to display the WMM service status. The EDCA parameters of the client that already take effect and the EDCA parameters used for the AP are not displayed when they adopt default settings.
- Obtain packets to display the EDCA parameters of the client.

Configuration Example

↘ Configuring WMM Service Parameters

Configuration Steps	● Enable or disable the WMM service on the AP. ● Configure EDCA parameters for the client. ● Configure EDCA parameters for the AP.
	Ruijie # configure terminal Hostname(config)# interface dot11radio 1/0 Hostname(config-if-Dot11radio 1/0)# wmm enable Hostname(config-if-Dot11radio 1/0)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 Hostname(config-if-Dot11radio 1/0)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50
Verification	Run the **show running** command to display the EDCA parameters of the client that already take effect and the EDCA parameters used for the AP. These parameters are not displayed when they adopt default settings.

Common Errors

- The performance is affected if EDCA parameters are improperly configured. For example, if the value of a low-priority parameter is higher than that of a high-priority parameter, the performance of the high priority is affected.

1.4.2 Configuring the QoS Packet Priority Mapping

Configuration Effect

- Configure packet priority mapping for the current WLAN.
- Configure 802.11p QoS mapping policy mechanism.
- Configure DSCP QoS mapping policy mechanism.

Notes

- QoS packet priority mapping takes effect after the WMM service is enabled.

Configuration Steps

By default, the mapping from DSCP to 802.11e is as follows.

DSCP	802.11e
0-7	0
16-23	1
24-31	2
8-15	3
32-39	4
40-47	5

48-55	6
56-63	7

By default, the mapping from 802.11e to DSCP is as follows:

802.11e	DSCP
0	0
3	8
1	16
2	24
4	32
5	40
6	48
7	56

Configuring Packet Priority Mapping for the WLAN

- Optional.
- Unless otherwise specified, packet priority mapping of the current WLAN shall be configured on all APs.

After the priority mapping and the value corresponding to the mapping table are set, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Command	**wlan-qos map-table** { **dot11e-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*
Parameter Description	**dot11e-dscp**: sets priority mapping from dot11e to internal DSCP. **dscp-dot11e**: sets priority mapping from dscp to dot11e. **import** *import-tag-value*: sets the priority of incoming original packets. **export** *export-tag-value*: sets priority of outgoing packets. **no**: restores the default packet mapping.
Command Mode	WLAN configuration mode
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled.

Enabling 802.11p QoS Mapping Policy Mechanism

- Optional.
- Unless otherwise specified, DSCP QoS mapping policy mechanism shall be disabled on all APs.

When the 802.11p QoS policy mechanism is enabled, the mapping table related to 802.11p QoS is used. When the 802.11p QoS policy mechanism is disabled, the default mapping policy is adopted.

Command	**wmm dot1p enable**
Parameter Description	N/A
Command Mode	Dot11radio interface configuration mode.
Usage Guide	This command is a mapping command for non-interworking versions.

	The parameter configuration takes effect only when the WMM service is enabled.

Configuring How to Apply the 802.11p QoS Mapping Policy Mechanism for the AP

- Optional.
- Unless otherwise specified, the 802.11p QoS mapping policy mechanism application shall be performed on all APs.

Determine where shall the 802.1Q priority be obtained based on the configuration determining how the AP applies the 802.11p QoS mapping policy mechanism.

Command	**wmm dot1p policy 1q** *1q-policy-value*
Parameter Description	*1q-policy-value*: indicates that the 802.11p QoS mapping policy mechanism is used. The value is 0 or 1. The default is 0.
Command Mode	Interface configuration mode
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled. The configuration for applying the 802.11p QoS mapping policy mechanism takes effect only when the 802.11p QoS mechanism is enabled.

Configuring 802.1p Priority

- Optional.
- Unless otherwise specified, 802.1p priority shall be configured on all APs.

Determine the priority of 802.1p based on the configuration of 802.1p priority.

Command	**wmm dot1p tag** *tag-value* { **back-ground** | **best-effort** | **video** | **voice** }
Parameter Description	**tag** *tag-value*: indicates the 802.1p priority. The value ranges from 0 to 7. The default **best-effort** is 0; the default ;**back-ground** is 2; the default **video** is 4; the default **voice** is 6. **back-ground**: indicates the back-ground queue. **best-effort**: indicates the best-effort queue. **video**: indicates the video queue. **voice**: indicates the voice queue.
Command Mode	Dot11radio interface configuration mode.
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled. The 802.1p priority configuration takes effect only when the 802.11p QoS mechanism is enabled.

Enabling DSCP QoS Mapping Policy Mechanism

- Optional.
- Unless otherwise specified, DSCP QoS mapping policy mechanism shall be disabled on all APs.

When the DSCP QoS policy mechanism is enabled, the mapping table related to DSCP QoS is used. When the DSCP QoS policy mechanism is disabled, the default mode is adopted for mapping.

Command	**wmm dscp enable**
Parameter Description	N/A
Defaults	DSCP QoS is disabled by default.
Command Mode	Dot11radio interface configuration mode.
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled.

Configuring How to Apply the DSCP QoS Mapping Policy Mechanism for the AP

- Optional.
- Unless otherwise specified, the DSCP QoS mapping policy mechanism application shall be performed on all APs.

Determine where shall the DSCP domain priority be obtained based on the configuration determining how the AP applies the DSCP QoS mapping policy mechanism.

Command	**wmm dscp policy outer-tunnel** *outer-tunnel-value* **inner-tunnel** *inner-tunnel-value*
Parameter Description	**outer-tunnel** *outer-tunnel-value*: indicates how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header. Value range: 0-1. The default is 0. **inner-tunnel** *inner-tunnel-value*: indicates how to apply the DSCP QoS mapping policy mechanism for the inner tunnel header. Value range: 0-1. The default is 0.
Command Mode	Dot11radio interface configuration mode.
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled. The configuration for applying the DSCP QoS mapping policy mechanism takes effect only when the DSCP QoS mechanism is enabled.

Configuring DSCP Identification

- Optional.
- Unless otherwise specified, DSCP identifications shall be configured on all APs.

Determine the DSCP priority based on the configured DSCP identifications.

Command	**wmm dscp tag** *tag-value* { **back-ground** | **best-effort** | **video** | **voice** }
Parameter Description	*tag-value*: indicates the DSCP priority. The value ranges from 0 to 63. The default best-effort is 0; the default **back-ground** is 16; the default video is 32; the default voice is 48. **back-ground**: indicates the back-ground queue. **best-effort**: indicates the best-effort queue. **video**: indicates the video queue. **voice**: indicates the voice queue.
Command Mode	Dot11radio interface configuration mode.
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled.

	DSCP identification configuration takes effect only when the DSCP mechanism is enabled.

Verification

- You can run the **show running** command to display the mapping configuration information. When the default configuration is adopted, no configuration information is displayed in the command output.
- Capture packets to check whether the priority mapping is correct.

Configuration Example

Configuring the QoS Packet Priority Mapping

Scenario	
	Connect AP001 to the L2 switch. Connect STA to AP001 in wireless mode, and connect the PC to the L2 switch.
Configuration Steps	Perform the following configuration on the AP: ● Enter the specified WLAN configuration mode. ● Configure the packet priority mapping.
	Hostname# configure terminal Hostname(config)# dot11 wlan 1 Hostname(dot11-wlan-config)# wlan-qos map-table dot11e-dscp import 7 export 50
Verification	Import AC_VO priority traffic in the direction from the STA to PC by using IxChariot, capture packets on the air interface, and display the priority at the wireless end. Then, capture packets from PC using a packet capturing tool to display the priority at the wired end.

Common Errors

- The WMM service is disabled.

1.5 Monitoring

Clearing

N/A

Displaying

N/A

Debugging

N/A

Configuring Wireless Optimization and Maintenance

1. Configuring WLOG
2. Configuring DATA-PLANE
3. Configuring METRICS-MONITOR

1 Configuring WLOG

1.1 Overview

WLOG (WLAN Log) enables storing and viewing wireless network and STA status in a past period of time. By collecting and storing the information of wireless network, AP and STA in the past 24 hours and then displaying the information through CLI commands, WLOG allows users to analyze the wireless network status and troubleshoot problems.

WLOG is for collecting and storage information, but does not support automatic information analysis temporarily. The WLOG feature is dedicated to enabling users, with provided information, to have a more accurate understanding of the wireless network and STA status in the past 24 hours to analyze and troubleshoot problems.

Protocols and Standards

- N/A

1.2 Applications

Application	Description
Fat AP Networking	Fat AP networking involves at least one AP and one STA.

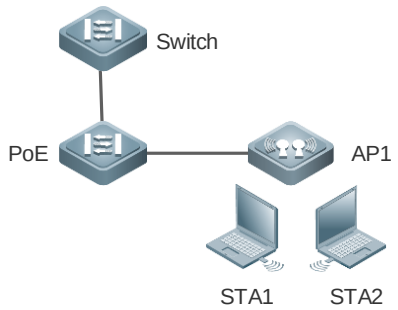
1.2.1 Fat AP Networking

Scenario

On a WLAN network, a fat AP is deployed to query the associated STAs.

The following example displays the STAs associated with the AP.

Figure 1-1



Note PoE: PoE switch, working as the gateway of the AP
AP: wireless access device
STA1 and STA2: user devices, working as STAs

Deployment

- Enable WLOG on the AP.

1.3 Features

Basic Concepts

The general information on the STA includes:

1. IP address
2. Signal strength
3. Access rate
4. Associated AP, radio and SSID

STA's spatial information

- The STA's spatial information mainly includes the statistics of data frame and management frame of the STA, as well as the statistics of each type of rate, as detailed below:

5. Number of data frames successfully transmitted (from the AP to the STA)/total traffic
6. Number of unresponsive data frames/total traffic
7. Number of management frames/total traffic
8. Statistics of each type of frames with access rate (The access rate is divided into 8 grades for statistics)

Grade	0	1	2	3	4	5	6	7
Access Type (Mbps)	1/2	5.5/11	6/9	12/18	24/36	48/54	Reserved	Reserved

9. Statistics of each type of frame with MIMO rate (The MIMO rate is divided into 8 grades for statistics)

Grade	0	1	2	3	4	5	6	7
MIMO Type	mcs0 mcs1	mcs2 mcs3	mcs4 mcs5	mcs6 mcs7	mcs8 mcs9	mcs10 mcs11	mcs12 mcs13	mcs14 mcs15

The spatial information is mainly used to check whether the STA is in low-speed state, whether the proportion of the case in which no ACK frame is transmitted is too high, and whether too many management frames are transmitted and received, so as to further analyze and locate the network problems caused by low speed node, management frame attack, and poor condition. The STA's spatial information varies in real time, and the current collection frequency is once every five minutes. The information is saved only on the AP due to large data volume.

STA Behaviors

STA behaviors include association, de-association, roaming, and login and logout upon web authentication and 802.1X authentication.

Features

Features	Purpose
Enabling WLOG_开启WLOG功能	Enables WLOG to obtain STA information automatically.
Configuring AP Sniffing	The AP detects STAs and hotspots around.

1.3.1 Enabling WLOG

After the WLOG feature is enabled, the AP automatically collects STA information and records the information into memory, enabling users, with provided information, to have a more accurate understanding of the wireless network and STA status in the past 24 hours and analyze and troubleshoot problems.

Working Principle

After the WLOG feature is enabled, the AP automatically collects STA information and records the information into memory, and receives online/offline advertisement of the STA and records into memory for users to view.

1.3.2 Configuring AP Sniffing

The AP sniffing function is used to detect STAs and hotspots around an AP. The AP sniffing function can be configured to detect either or both of STAs and hotspots.

Working Principle

After the AP in the Fat mode is enabled with sniffing, sniffing information is output in syslogs.

1.4 Configuration

Configuration	Description and Command	
Enabling WLOG	⚠ (Mandatory) It is used to enable the WLOG feature.	
	wlan diag enable	Enables the WLOG feature
Configure AP Sniffing	⚠ (Optional) It is used to enable AP sniffing.	
	ap-probe ap enable	Enables the hotspot information probe function of an AP.
	ap-probe sta enable	Enables the STA information probe function of an AP.
	ap-probe cache-time	Configures the time for caching detected information (aging) for an AP.
	ap-probe upload-time	Configures the interval for periodically outputting logs of detected information for an AP.
	ap-probe limit	Configures the number of non-repetitive detected information records that can be received within aging period for the AP.

1.4.1 Enabling WLOG

Configuration Effect

- After the WLOG feature is enabled, the AP automatically records the STA information.

Notes

- Enabling the WLOG feature pre-allocates memory. If the memory is not sufficient, the WLOG feature cannot be enabled. Disabling the WLOG feature frees all memory for information storage and pre-allocated memory.

Configuration Steps

↘ Enabling the WLOG Feature

- (Mandatory) Run the **wlog diag enable** command to enable the WLOG feature.
- After the WLOG feature is enabled, information is collected and recorded into memory on a regular basis.

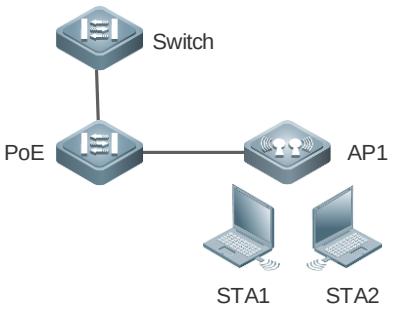
Command	**wlan diag enable**
Parameter Description	-
Defaults	By default, the WLOG feature is disabled on the AP device.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show wlan diag sta** command to check whether the STA information can be viewed on the AP.

Configuration Example

↘ Enabling WLOG

Scenario Figure 1-1	
Configuration Steps	● Enable WLOG in global configuration mode.
RADIUS Client	Hostname# configure terminal

	Hostname(config)# wlan diag enable
Verification	Run the **show wlan diag sta** command to display the WLOG status.
	Hostname# show wlan diag sta sta mac: c83a.35c6.0c72 ========== ========== ========== 2012-05-28 19:31:08 wlan id state rssi_rt rs_rate_mcs tx_frm_cnts rx_frm_cnts tx_frm_flow rx_frm_flow tx_cnts_error tx_flow_error mgmt_cnts mgmt_flow -------- -------- -------- ---------- ---------- ---------- ---------- ---------- ---------- --------- --------- 1 3 23 80 18 59 4384 5967 0 0 3 381 tx/rxmcs mcs0, mcs1 mcs2, mcs3 mcs4, mcs5 mcs6, mcs7 mcs8, mcs9 mcs10, mcs11 mcs12, mcs13 mcs14, mcs15 ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- txmcspercent : 0 0 0 0 0 0 0 0 rxmcspercent : 0 0 0 0 0 0 0 0 tx/rxrate 1, 2 5.5, 11 6, 9 12, 18 24, 36 48, 54 -- -- ---------- ------- ------- ------- ------- ------- ------- ------- ------- txratepercent: 16 0 0 7 50 27 0 0 rxratepercent: 57 3 0 5 13 22 0 0

Common Errors

- N/A

1.4.2 Configure AP Sniffing

Configuration Effect

After an AC delivers the command to enable AP sniffing, the AP periodically reports detected STA information and hotspot information to the AC.

Configuration Steps

Enabling the Hotspot Information Probe Function of an AP

- Optional. After the function is enabled, an AP can detect hotspot information.

Command	**ap-probe ap enable**
Parameter Description	*N/A*
Defaults	This function is not configured by default.
Command Mode	AP configuration mode, and all-AP configuration mode
Usage Guide	N/A

Enabling the STA Information Probe Function of an AP

- Optional. After the function is enabled, an AP can detect STA information.

Command	**ap-probe sta enable**
Parameter Description	N/A
Defaults	This function is not configured by default.
Command Mode	AP configuration mode, and all-AP configuration mode
Usage Guide	N/A

Configuring the Time for Caching Detected Information (Aging) for an AP

- Optional. Configure the time for caching detected information by an AP on the AP.

Command	**ap-probe cache-time** *time*
Parameter Description	*time*: Indicates the cache time(aging time). The value ranges from 0 to 3,600 seconds.
Defaults	The default value is 120 seconds.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	When the cache time is set to 0 seconds, the AP does not cache data, resulting in a large amount of logs of duplicate information being outputted. The packet sending frequency is too high, which may cause the CPU load of the AP to be excessively high and potentially impact wireless services. We recommend you to use this configuration only during environment debugging, and it is not recommended to set the cache time to 0 seconds under normal service conditions.

Configuring the Interval for Periodically Outputting Logs of Detected Information for an AP

- Optional. Configure the interval for periodically outputting logs of detected information for an AP.

Command	**ap-probe upload-time** *time*
Parameter Description	*time*: Indicates the interval for periodically outputting logs of detected information. The value ranges from 1 to 300 seconds.

Defaults	The default value is 5 seconds.
Command Mode	AP configuration mode, and all-AP configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Detected Information Records That Can Be Cached on an AP

- Optional. Configure the number of non-repetitive detected information records that can be received within the aging period for the AP.

Command	**ap-probe limit** *num*
Parameter Description	*num*: Indicates the number of detected information records that can be cached on an AP. The value ranges from 1 to 65,535 The actual number of records that can be cached on an AP depends on the size of the AP's memory.
Defaults	The default value is 100.
Command Mode	AP configuration mode, and all-AP configuration mode
Usage Guide	If the configured value of *num* exceeds the maximum number of information records supported by an AP, the maximum number of information records supported by the AP prevails. Cached information occupies certain memory resources. Therefore, it is not recommended to set it to a large number.

Verification

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

Configuration Example

Enabling the Sniffing of AP

Configuration Steps	• Enable the hotspot and STA probe function in AP configuration mode. Set the cache time to 60 seconds, the interval of outputting logs to 6 seconds, and the number of non-repetitive detected information that can be cached to 200.
AP	Hostname# configure terminal Hostname(config)# ap-probe ap enable Hostname(config)# ap-probe sta enable Hostname(config)# ap-probe cache-time 60 Hostname(config)# ap-probe upload-time 6 Hostname(config)# ap-probe limit 200 Hostname(config)#
Verification	Run the **show ap-config running | include ap-probe** command to display the configuration.
AP	Hostname# show running-config| include ap-probe ! ap-probe sta enable ap-probe ap enable ap-probe upload-time 6

	ap-probe cache-time 60 ap-probe limit 200 !

1.5 Monitoring

Displaying

Description	Command
Displays the STA information on the AP	**show wlan diag sta** [**sta-mac** *sta-mac*] [**number** *number*]

1 Configuring DATA-PLANE

1.1 Overview

The data plane provides broadcast forwarding control functions, including broadcast forwarding weight control and broadcast wireless forwarding control.

Broadcast forwarding weight control means restricting the weights of packet types for broadcast forwarding, so as to prevent STAs from being influenced when a certain type of packets occupy all resources.

Broadcast wireless forwarding control means forwarding only necessary packets to the wireless network, so as to prevent some useless broadcast packets from occupying substantial radio frequency (RF) resources.

- Broadcast forwarding weight control is applicable to all packets to be flooded.
- Broadcast wireless forwarding control is applicable to all packets to be sent to the radio interface.

Protocols and Standards

- N/A

1.2 Applications

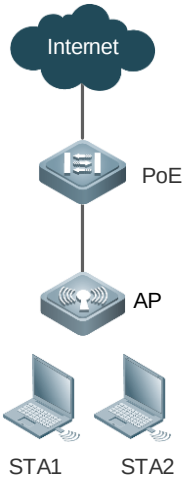
Application	Description
Controlling Broadcast Packets Sent to the Wireless Network	Fat AP networking is used, which includes at least one switch and one AP.

1.2.1 Controlling Broadcast Packets Sent to the Wireless Network

Scenario

On a wireless network, deploy an AP to control broadcast packets sent to the wireless network, as shown in Figure 1-1.

Figure 1-1



Remarks	PoE: switch, used as the gateway of the AP. AP: wireless access point STA1 and STA2: wireless stations

Deployment

Enable the function of controlling broadcast packets sent to the wireless network on the AP.

1.3 Features

Basic Concepts

Broadcast Forwarding Weight Control

A network switching device may need to flood broadcast packets, multicast packets, and some unicast packets. A weight can be set for each type of packets to prevent a certain type of broadcast packets from exhausting all broadcast forwarding capabilities, thereby improving STAs' network experience.

Broadcast Wireless Forwarding Control

The broadcast wireless forwarding control function is used to forward only necessary broadcast packets to the wireless network, so as to prevent certain broadcast packets from occupying substantial air interface resources and improve the network rates of STAs.

ARP Broadcast Control

In some scenarios, intra-LAN ARP discovery is not allowed. That is, users on the LAN do not respond to ARP requests from the external network, thereby achieving isolation and preventing ARP scanning (host discovery). Users on the LAN are also mutually isolated.

ARP or ND Broadcast Isolation Between CAPWAP tunnel interfaces

CAPWAP tunnel interfaces do not broadcast ARP or ND packets to each other by default. Run the command to enable CAPWAP tunnel interfaces to mutually broadcast ARP or ND packets.

Allowing Multicast DNS (mDNS) Packets to Pass Through

Wireless broadcast forwarding does not allow mDNS packets to pass through by default. In some scenarios such as screen mirroring, the mDNS keepalive packets from the screen end to the terminal are blocked by

the device, causing a mirroring disconnection. To restore mirroring, configure the device to allow the mDNS packets to pass through.

↘ Allowing Simple Service Discovery Protocol (SSDP) Packets to Pass Through

Wireless broadcast forwarding does not allow SSDP packets to pass through by default. Run the command to configure the device to allow SSDP packets to pass through as required.

↘ Allowing Open Shortest Path First (OSPF) Packets to Pass Through

Wireless broadcast forwarding does not allow OSPF packets to pass through by default. In some scenarios, an AP may be connected to an OSPF network instead of an end STA. In this case, the device needs to allow OSPF packets to pass through.

↘ Allowing Virtual Router Redundancy Protocol (VRRP) Packets to Pass Through

Wireless broadcast forwarding does not allow VRRP packets to pass through by default. Run the command to configure the device to allow VRRP packets to pass through as required.

Overview

Feature	Description
Broadcast Forwarding Weight Control	Restricts the weights of packet types for broadcast forwarding, so as to protect RF resources from being occupied by a certain type of packets and thereby guarantee normal forwarding of other packets.
Broadcast Wireless Forwarding Control	Controls whether to forward broadcast packets to the wireless network, so as to prevent useless broadcast packets from occupying substantial RF resources.
ARP Broadcast Control	Prevents ARP discovery and ARP scanning on a LAN.
Downlink Wired and Wireless User Isolation	Blocks ARP packets between downlink wired and wireless users to achieve wireless and wired user isolation.
ARP or ND Broadcast Isolation	Configures the device to mutually broadcast ARP or ND packets between CAPWAP tunnel interfaces.
mDNS Packet Control	Configures the device to allow mDNS packets to pass through.
SSDP Packet Control	Configures the device to allow SSDP packets to pass through.
OSPF Packet Control	Configures the device to allow OSPF packets to pass through.
VRRP Packet Control	Configures the device to allow VRRP packets to pass through.
Intra-VLAN STA isolation	Enables intra-VLAN STA isolation.

1.3.1 Broadcast Forwarding Weight Control

Broadcast forwarding weight control is used to restrict a certain type of packets, so that the ratio of this type of packets is no greater than the specified weight during broadcast forwarding.

Working Principle

The broadcast forwarding weight control function classifies packets at first into unicast packets, multicast packets, broadcast packets, unknown multicast packets, and unknown unicast packets.

- Classify packets. Packets may be roughly classified into the following types: unicast packets, multicast packets, broadcast packets, unknown multicast packets, and unknown unicast packets.
- Allocate a token bucket to each type of packets, and record the number of packets permitted to pass at this moment.
- According to the configured broadcast forwarding weights, calculate the number of packets permitted to pass within each interval, and adjust the sizes of the token buckets accordingly.
- When a packet arrives, determine the type of the packet and check whether there is any token in the token bucket corresponding to the packet type. If the token bucket contains a token, the packet is permitted to pass; otherwise, the packet is discarded.

1.3.2 Broadcast Wireless Forwarding Control

The broadcast wireless forwarding control function is used to forward only partial packets that affect STAs to the wireless network, so as to prevent useless broadcast packets from occupying substantial air interface resources.

Working Principle

Wireless networks differ from wired networks in performance. In a wireless network, air interface resources are shared by STAs and APs which often becomes a bottleneck for STAs. Meanwhile, they are seized for a long time because broadcast packets are sent at low rates.

In practice, some broadcast packets are useless for STAs. Forwarding these packets to the wireless network will result in fewer air interface resources and worse user experience.

One solution is to classify broadcast packets for forwarding control. Only the packets of specified types are forwarded to the wireless network.

1.3.3 ARP Broadcast Control

Parse ARP packets to control uplink and downlink ARP packet forwarding.

Principles

In some scenarios, ARP discovery and ARP scanning on a LAN are not allowed.

APs in the MACC scenario support ARP isolation. That is, the uplink ARP packets are forwarded except those from a radio port or LAN port and the downlink ARP packets are not forwarded except those containing the trusted source IP address.

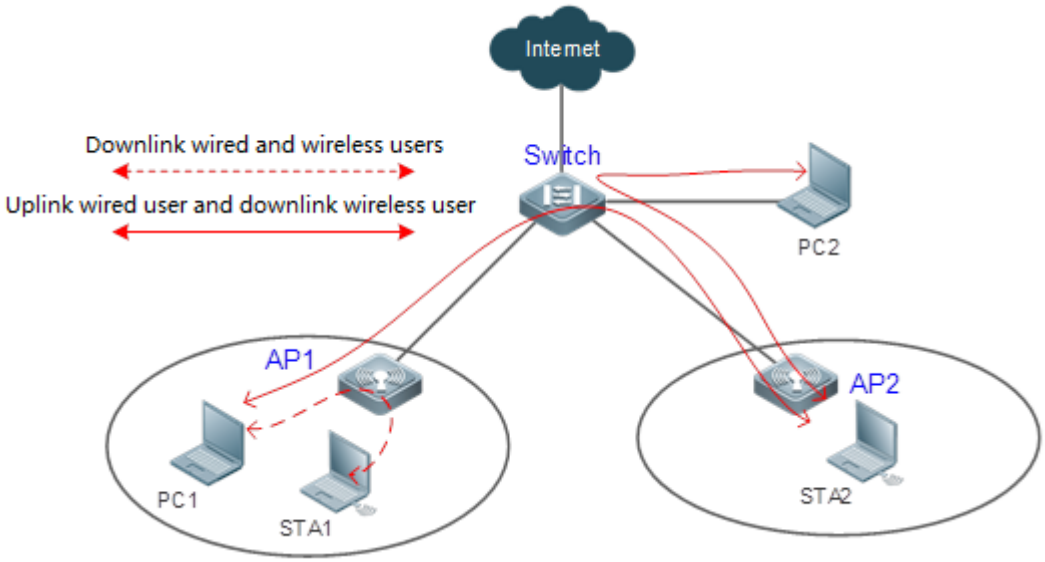
1.3.4 Downlink Wired and Wireless User Isolation

In fat AP networking scenarios, there are two types of links between wired and wireless users:

1. Link between downlink wired and wireless users

2. Link between uplink wired and downlink wireless users

Figure 1-2 Link Between Wired and Wireless Users



In some scenarios, the network administrator wants to block the former link type to ensure network security. The network administrator can achieve wired and wireless user isolation by blocking ARP packet transmission between downlink wired and wireless users.

Working Principle

On the fat AP, control ARP forwarding based on the source and destination interfaces of ARP broadcast packets.

ARP packets are not forwarded in the following two cases:

1. The source interface is a downlink wired interface and the destination interface is a wireless interface.
2. The source interface is a wireless interface and the destination interface is a downlink wired interface.

1.3.5 ARP or ND Broadcast Isolation

ARP or ND broadcast isolation between CAPWAP tunnel interfaces are enabled by default. ARP or ND packets are not broadcast to CAPWAP tunnel interfaces directly. Instead, the gateway responds the APR and ND broadcast packets through ARP or ND proxy. In some scenarios with ARP or ND proxy disabled, STAs in a VLAN may fail to ping each other due to broadcast isolation.

Working Principle

In some scenarios with ARP or ND proxy disabled, to allow successful ping among STAs in a VLAN, you can run the command to disable ARP or ND broadcast isolation between CAPWAP tunnel interfaces.

1.3.6 mDNS Packet Control

When wireless broadcast forwarding is disabled, mDNS packets are not sent to the CAPWAP tunnel interface by default. You can run the command to send mDNS packets to the CAPWAP tunnel interface.

Working Principle

In some scenarios with wireless broadcast forwarding disabled, you can run the command to send mDNS packets to the CAPWAP tunnel interface.

1.3.7 SSDP Packet Control

When wireless broadcast forwarding is disabled, SSDP packets are not sent to the CAPWAP tunnel interface by default. You can run the command to send SSDP packets to the CAPWAP tunnel interface.

Working Principle

In some scenarios with wireless broadcast forwarding disabled, you can run the command to send SSDP packets to the CAPWAP tunnel interface.

1.3.8 OSPF Packet Control

OSPF packets are not sent to the CAPWAP and roaming tunnel interfaces by default. You can run the command to send OSPF packets to the CAPWAP and roaming tunnel interfaces.

Working Principle

In some scenarios with wireless broadcast forwarding disabled, you can run the command to send OSPF packets to the CAPWAP and roaming tunnel interfaces.

1.3.9 VRRP Packet Control

VRRP packets are not sent to the CAPWAP and roaming tunnel interfaces by default. You can run the command to send VRRP packets to the CAPWAP and roaming tunnel interfaces.

Principles

In some scenarios with wireless broadcast forwarding disabled, you can run the command to send VRRP packets to the CAPWAP and roaming tunnel interfaces.

1.3.10 Intra-VLAN STA isolation

By default, STAs in a VLAN are isolated from each other and can communicate with their gateways only. However, you can add devices to an allowlist to allow them to communicate with STAs in the VLAN.

Working Principle

If intra-VLAN STA isolation is enabled on a fat AP, the AP forwards DHCP and ARP packets of STAs to discover their gateways. That is, STAs can communicate with their gateways by default but cannot communicate with each other. You can also add devices to an allowlist to enable them to communicate with STAs in the VLAN.

1.4 Configuration

Configuration	Description and Command	
Configuring the Broadcast Forwarding Weight	⚠ (Optional) Set the weights of packet types for broadcast forwarding.	
	data-plane queue-weight	Configures the weights of packet types for broadcast forwarding on the AP.
	data-plane token	Configures the refresh interval of the broadcast token bucket and bucket-based rate on the AP.
Configuring Broadcast Wireless Forwarding	⚠ (Optional) Enable the broadcast wireless forwarding function.	
	data-plane wireless-broadcast	Enables or disables the broadcast wireless forwarding control function on the AP.
Configuring ARP Broadcast Control	⚠ (Optional) Enable ARP broadcast control to prevent ARP discovery in a LAN.	
	data-plane arp-control enable	Enables or disables ARP broadcast control.
	data-plane arp-control vlan	Configures a trusted host for ARP broadcast control.
Isolating Wired and Wireless STAs Connected with an AP	⚠ (Optional) It is used to forbid ARP discovery between a LAN and a WLAN, ensuring network isolation.	
	data-plane lan-ssid-control enable	Enables or disables LAN-WLAN isolation.
Configuring ARP or ND Broadcast Isolation	⚠ (Optional) It is used to control ARP or ND broadcast between CAPWAP tunnel interfaces.	
	data-plane close-arp-filter	Broadcasts ARP packets to the CAPWAP tunnel interface.
	data-plane close-nd-filter	Broadcasts ND packets to the CAPWAP tunnel interface.
Configuring the Device to Allow Specified Packets to Pass Through	⚠ (Optional) It is used to allow mDNS, SSDP, OSPF, or VRRP packets to pass through.	
	data-plane close-mdns-filter	Allows mDNS packets to pass through when wireless broadcast forwarding is disabled.

	data-plane close-ssdp-filter	Allows SSDP packets to pass through when wireless broadcast forwarding is disabled.
	data-plane close-ospf-filter	Allows OSPF packets to pass through when wireless broadcast forwarding is disabled.
	data-plane close-vrrp-filter	Allows VRRP packets to pass through when wireless broadcast forwarding is disabled.
Enabling Intra-VLAN STA Isolation	⚠ (Optional) It is used to forbid communication between STAs in a VLAN, ensuring network isolation between the STAs.	
	data-plane user-isolation vlan	Enables or disables intra-VLAN user isolation.
	data-plane user-isolation trusted-mac	Adds or deletes a trusted MAC address.
	data-plane user-isolation trusted-ip	Adds or deletes a trusted IPv4 address.

1.4.1 Configuring the Broadcast Forwarding Weight

Networking Requirements

- You can control the weight of a packet type for forwarding according to actual network conditions, so as to avoid network congestion for sudden traffic spike.

Notes

- N/A

Configuration Steps

↘ Configuring the Broadcast Forwarding Weight

- Optional. Run the **data-plane queue-weight** command to configure the broadcast forwarding weights.

Command	**data-plane queue-weight** *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*
Parameter Description	*unicast-packet-weight*: Sets the forwarding weight of unicast packets. The range is from 1 to 100. The default weight is 16. *multicast-packet-weight*: Sets the forwarding weight of multicast packets. The range is from 1 to 50. The default weight is 4. *broadcast-packet-weight*: Sets the forwarding weight of broadcast packets. The range is from 1 to 50. The default weight is 2. *unknown-multicast-packet-weight*: Sets the forwarding weight of unknown multicast packets. The range is from 1 to 25. The default weight is 8. *unknown-unicast-packet-weight*: Sets the forwarding weight of unknown unicast packets. The range is from 1 to 25. The default weight is 1.
Defaults	Default weights are applied.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Refresh Interval of Broadcast Token Bucket and Bucket-based Rate

- Optional. Run the **show run** command to display the configuration.

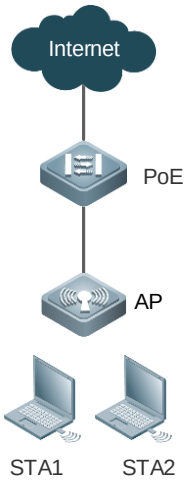
Command	**data-plane token** *token-interval token-base-rate*
Parameter Description	*token-interval*: Refresh interval of broadcast token bucket in 10 ms. The default interval is 1. The value ranges from 1 to 10,000. token-base-rate: Broadcast token rate. The value ranges from 1 to 1,000,000. The default value is 5.
Defaults	Default parameters are applied.
Command Mode	Global configuration mode
Usage Guide	Broadcast rate per second = Packet weight × (1s/Refresh Interval) x Token bucket-based rate

Verification

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

Configuration Example

Configuring the Broadcast Weight

Scenario **Figure 1-1**	
Configuration Steps	● Configure the weight of broadcast packets in global configuration mode.
AP	Hostname#configure terminal Hostname(config)#data-plane queue-weight 100 50 50 25 25 Hostname(config)#data-plane token 10 10 Hostname(config)#exit
Verification	Run the **show run** command to display the configuration.
	Hostname# show running ... ! cwmp !

Common Errors

- N/A

1.4.2 Configuring Broadcast Wireless Forwarding

Networking Requirements

- Useless broadcast packets are not forwarded to the air interface.

Notes

- N/A

Configuration Steps

Broadcast Forwarding Function

- Optional. By default, the broadcast wireless forwarding function is disabled. Run the data-plane wireless-broadcast command in global configuration mode to enable or disable this function.

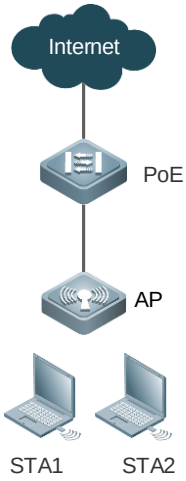
Command	**data-plane wireless-broadcast**{ **enable** | **disable** }
Parameter Description	**enable**: Allows all broadcast packets to be forwarded to the air interface. **disable**: Prevents all broadcast packets from being forwarded to the air interface.
Defaults	The broadcast wireless forwarding function is disabled; that is, broadcast packets are not forwarded to the wireless network.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Enabling Wireless Broadcast Forwarding

Scenario	
Figure 1-2	
Configuration Steps	• Enable wireless broadcast forwarding in global configuration mode.
AP	Hostname#configure terminal Hostname(config)#data-plane wireless-broadcast enable
Verification	Run the **show running-config** command to display the configuration.
AP	Hostname# show ap-config running ! cwmp ! data-plane wireless-broadcast enable

	!

Common Errors

- N/A

1.4.3 Configuring ARP Broadcast Control

Configuration Effect

- Prevent ARP discovery and ARP scanning on a LAN.

Notes

- N/A

Configuration Steps

↘ Enabling ARP Broadcast Control

- (Optional)
- Configure this function if you want to prevent ARP discovery and ARP scanning on a LAN.
- In MACC scenarios, configure this command in AP global configuration mode.

Command	**data-plane arp-control enable**
Parameter Description	**enable**: Enables ARP broadcast control to prevent ARP discovery and ARP scanning on a LAN.
Defaults	ARP broadcast control is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Trusted Host for ARP Broadcast Control

- Optional.
- Configure this command if you want to allow the specified host to discover the device on the LAN.
- In MACC scenarios, configure this command in global configuration mode.

Command	**data-plane arp-control vlan** *vlan-id* **trusted-host** *ipv4-address*
Parameter Description	*vlan-id*: ID of the VLAN to be enabled with ARP broadcast control. The value ranges from 1 to 4094. *ipv4-address*: Trusted IP address. Up to 64 IP addresses are allowed.
Defaults	No trusted IP address is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

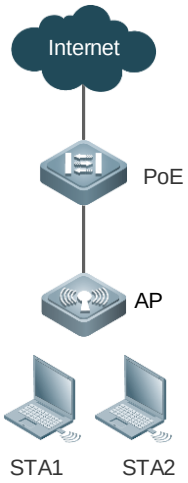
- Run the **show running** command to display the configuration.

Configuration Example

↘ Enabling ARP Broadcast Control

Scenario

Figure1-3



Configuration Steps AP

Enable ARP broadcast control in global configuration mode.

```
Hostname#configure terminal
Hostname(config)# data-plane arp-control enable
```

Verification AP

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

```
Hostname# show running
!
cwmp
!
data-plane arp-control enable
!
```

Common Errors

- N/A

1.4.4 Isolating Wired and Wireless STAs Connected with an AP

Configuration Effect

Wired and wireless STAs connected with an AP are not allowed to discover each other through ARP packets, ensuring network isolation.

Notes

N/A

Configuration Steps

Isolating Wired and Wireless STAs Connected with an AP

- Optional.
- Run the **data-plane lan-ssid-control enable** command in global configuration mode.

Command	**data-plane lan-ssid-control enable**
Parameter Description	N/A
Defaults	Wired and wireless STAs connected with an AP are not isolated by default.
Command Mode	Global configuration mode
Usage Guide	This command is used to forbid wired and wireless STAs connected with an AP from discovering each other through ARP packets, ensuring network isolation.

Verification

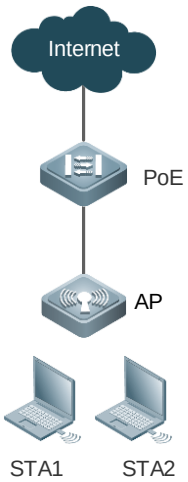
Run the **show running-config** command to display the configuration.

Configuration Example

Isolating Wired and Wireless STAs Connected with an AP

Scenario

Figure 1-4



Configuration Steps	Enable the LAN-WLAN isolation function in global configuration mode.
AP	Hostnamee# configure terminal Hostnamee(config)# data-plane lan-ssid-control enable
Verification	Run the **show running-config** command to display the configuration.
AP	Hostnamee# show running-config !

```
data-plane lan-ssid-control enable
!
```

Common Errors

N/A

1.4.5 Configuring ARP or ND Broadcast Isolation

Configuration Effect

- Control whether to broadcast ARP or ND packets to the CAPWAP tunnel interface.

Notes

- N/A

Configuration Steps

Disabling ARP Broadcast Isolation

- Optional.
- ARP packets are not broadcast to the CAPWAP tunnel interface by default.
- Configure this function if you want to broadcast ARP packets to the CAPWAP tunnel interface.
- Configure this command in global configuration mode.

Command	**data-plane close-arp-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows ARP packets to be broadcast to the CAPWAP tunnel interface. **disable**: Prevents ARP packets from being broadcast to the CAPWAP tunnel interface.
Defaults	ARP packets are not broadcast to the CAPWAP tunnel interface by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling ND Broadcast Isolation

- Optional.
- ND packets are not broadcast to the CAPWAP tunnel interface by default.
- Configure this function if you want to broadcast ND packets to the CAPWAP tunnel interface.
- Configure this command in global configuration mode.

Command	**data-plane close-nd-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows ND packets to be broadcast to the CAPWAP tunnel interface. **disable**: Prevents ND packets from being broadcast to the CAPWAP tunnel interface.
Defaults	ND packets are not broadcast to the CAPWAP tunnel interface by default.
Command Mode	Global configuration mode

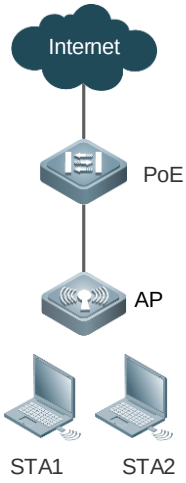
Usage Guide	N/A

Verification

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

Configuration Example

Disabling ARP Broadcast Isolation

Scenario Figure 1-5	
Configuration Steps	Disable ARP broadcast isolation in global configuration mode.
AP	Hostname#configure terminal Hostname(config)#data-plane close-arp-filter enable
Verification	Run the **show running-config** command to display the configuration.
AP	Hostname# show running ! cwmp ! data-plane close-arp-filter enable !

Common Errors

- N/A

1.4.6 Configuring the Device to Allow Specified Packets to Pass Through

Configuration Effect

- When wireless broadcast forwarding is disabled, allow mDNS, SSDP, OSPF, or VRRP packets to pass through.

Notes

- N/A

Configuration Steps

Configuring mDNS Packet Control

- Optional.
- mDNS packets are not allowed to pass through by default.
- Configure this function if you want to allow mDNS packets to pass through.
- Configure this command in global configuration mode.

Command	**data-plane close-mdns-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows mDNS packets to be forwarded to the air interface. **disable**: Prevents mDNS packets from being forwarded to the air interface.
Defaults	mDNS packets are not forwarded to the wireless network by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring SSDP Packet Control

- Optional.
- SSDP packets are not allowed to pass through by default.
- Configure this function if you want to allow SSDP packets to pass through.
- Configure this command in global configuration mode.

Command	**data-plane close-ssdp-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows SSDP packets to be forwarded to the air interface. **disable**: Prevents SSDP packets from being forwarded to the air interface.
Defaults	SSDP packets are not forwarded to the wireless network by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring OSPF Packet Control

- Optional.
- OSPF packets are not allowed to pass through by default.

- Configure this function if you want to allow OSPF packets to pass through.
- Configure this command in global configuration mode.

Command	**data-plane close-ospf-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows OSPF packets to be forwarded to the air interface. **disable**: Prevents OSPF packets from being forwarded to the air interface.
Defaults	OSPF packets are not forwarded to the wireless network by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring VRRP Packet Control

- Optional.
- VRRP packets are not allowed to pass through by default.
- Configure this function if you want to allow VRRP packets to pass through.
- Configure this command in global configuration mode.

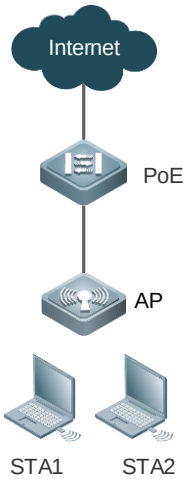
Command	**data-plane close-vrrp-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows VRRP packets to be forwarded to the air interface. **disable**: Prevents VRRP packets from being forwarded to the air interface.
Defaults	VRRP packets are not forwarded to the wireless network by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the AP to Allow OSPF Packets to Pass Through

Scenario Figure 1-6	

Configuration Steps	Configure the AP to allow OSPF packets to pass through in the global configuration mode.
AP	Hostname#configure terminal Hostname(config)#data-plane close-ospf-filter enable
Verification	Run the **show running-config** command to display the configuration.
AP	Hostname# show running ! cwmp ! data-plane close-ospf-filter enable !

Common Errors

- N/A

1.4.7 Enabling Intra-VLAN STA Isolation

Configuration Effect

By default, STAs in a VLAN cannot communicate with each other and can communicate with their gateways only. You can add the MAC addresses of devices that need to communicate with STAs in the VLAN to an allowlist.

Notes

- The IP DHCP snooping function must be enabled.
- STAs must obtain IP addresses through DHCP, and only IPv4 addresses are supported.
- The default gateway IP address must be configured for the DHCP address pool.
- When intra-VLAN user isolation is enabled, wireless STAs will be brought offline and wired STAs can access the network only after they obtain IP addresses through DHCP.

Configuration Steps

↘ Enabling Intra-VLAN STA Isolation

- Optional.

Command	**data-plane user-isolation vlan** *vid*
Parameter Description	*vid*: ID of the VLAN for which STA isolation is enabled. The range is from 1 to 4094.
Defaults	STAs in a VLAN are not isolated by default.

Command Mode	Global configuration mode
Usage Guide	1. To enable intra-VLAN STA isolation, you must enable IP DHCP snooping first. 2. The default gateway IP address must be configured for the DHCP address pool. 3. STA isolation can be enabled for a maximum of 16 VLANs on an AP.

Configuring an Allowlist

- Optional.

Command	**data-plane user-isolation** { **trusted-mac** *H.H.H* | **trusted-ip** *ipv4_address* } **vlan** *vid*
Parameter Description	*H.H.H*: MAC address of a STA to be allowed to communicate with other STAs in the VLAN. *ipv4_address*: IPv4 address of a STA to be allowed to communicate with other STAs in the VLAN. *vid*: ID of the VLAN for which STA isolation is enabled.
Defaults	STAs in a VLAN are not isolated by default.
Command Mode	Global configuration mode
Usage Guide	A maximum of 64 allowlists can be configured for intra-VLAN STA isolation on an AP.

Verification

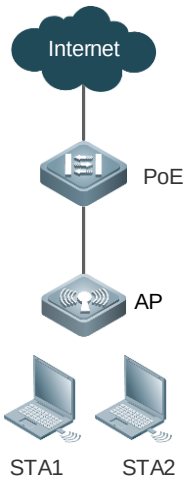
Run the **show running-config** command to display the configuration.

Configuration Example

Enabling STA Isolation for VLAN 10

Scenario

Figure 1-9



Configuration Steps	Configure the default gateway of AP1 on the PoE switch. In global configuration mode of AP1, add the STA whose MAC address is 0010.1111.2222 to the allowlist.
AP	Hostname# configure terminal Hostname(config)# data-plane user-isolation vlan 10 Hostname(config)# data-plane user-isolation trusted-mac 0010.1111.2222 vlan 10
Verification	Run the **show running-config** command to display the configuration.

AP

```
Hostname# show running-config
!
data-plane user-isolation vlan 10
data-plane user-isolation trusted-mac 0010.1111.2222 vlan 10
!
```

Common Errors

IP DHCP snooping is not configured.

1.5 Monitoring

Clearing

N/A

Displaying

Function	Command
Displays the configuration of intra-VLAN STA isolation.	**show data-plane user-isolation** { **summary** | **ap-group** *ap_group_name* }
Displays the allowlists configured for intra-VLAN STA isolation.	**show data-plane user-isolation state**

Debugging

N/A

1 Configuring METRICS-MONITOR

1.1 Overview

METRICS-MONITOR is developed to collect and monitor key data on an access controller (AC) or access point (AP), to improve the information collection and fault locating efficiency.

Protocols and Standards

N/A

1.2 Features

Overview

Feature	Description
METRICS-MONITOR	Commands can be run to display and clear data of a specified metric on a specified device.

1.2.1 METRICS-MONITOR

Working Principle

Wireless devices collect and record data of metrics defined in the system. CLI commands provided by the metrics module can display or clear data by metric group or metric name.

1.3 Configuration

Configuration	Description and Command	
Displaying and Clearing Metric Data	(Optional) Enable the broadcast wireless forwarding function.	
	metrics monitor enable	Enables metric monitoring on the device.
	clear metrics all	Clears all metric data.
	clear metrics group *group-name*	Clears data of all metrics in a specified metric group.
	clear metrics group *group-name metrics-name*	Clears data of a specified metric in a specified metric group.

1.3.1 Displaying and Clearing Metric Data

Configuration Effect

- Clear metric data collected by the device. The range of data to be cleared can be configured and may include all data, data of a specified group, and data of a specified metric in a specified group.

Notes

N/A

Configuration Steps

↘ Enabling Metric Monitoring on the Device

- Optional.
- In global configuration mode, enable metric monitoring on the device.

Command	**metrics monitor enable**
Parameter Description	N/A
Defaults	It is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Clearing All Metric Data

- Optional.
- In global configuration mode, clear all metric data collected by the device.

Command	**clear metrics all**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

↘ Clearing Data of All Metrics in a Specified Metric Group

- Optional.
- In global configuration mode, clear data of all metrics in a specified metric group on the device.

Command	**clear metrics group** *group-name*
Parameter Description	*group-name*: Indicates the name of a specified metric group.
Defaults	N/A

Command Mode	Privileged EXEC mode
Usage Guide	N/A

Clearing Data of a Specified Metric in a Specified Metric Group

- Optional.
- In global configuration mode, clear data of a specified metric in a specified metric group.

Command	**clear metrics group** *group-name metrics-name*
Parameter Description	*group-name*: Indicates the name of a specified metric group. *metrics-name*: Indicates the name of a specified metric.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- Run the **show metrics summary** command to display collected data.
- Run the **show metrics summary group** *group-name* command to display data of all metrics in a metric group.
- Run the **show metrics detail** *group-name metrics-name* command to display data of a specified metric in a metric group.

Configuration Example

Clearing Specified Data

Configuration Steps	1. Clear all metric data. 2. Clear data of all metrics in a metric group named **sys**. 3. Clear data of a metric named **memory** in a metric group named **sys**.
	Hostname# clear metrics all Hostname# clear metrics group sys Hostname# clear metrics group sys memory
Verification	1. Run the **show metrics summary** command to display collected data. 2. Run the **show metrics summary group** *group-name* command to display data of all metrics in a specified metric group. 3. Run the **show metrics detail** *group-name metrics-name* command to display data of a specified metric in a specified metric group. The following uses the **show metrics summary** command as an example. Run this command immediately after clearing metric data.
	Hostname# clear metrics all Hostname# show metrics summary group name unit tags value LastUpdTime

Configuration Steps	1. Clear all metric data. 2. Clear data of all metrics in a metric group named **sys**. 3. Clear data of a metric named **memory** in a metric group named **sys**.
	Hostname# clear metrics all Hostname# clear metrics group sys Hostname# clear metrics group sys memory
Verification	1. Run the **show metrics summary** command to display collected data. 2. Run the **show metrics summary group** *group-name* command to display data of all metrics in a specified metric group. 3. Run the **show metrics detail** *group-name metrics-name* command to display data of a specified metric in a specified metric group. The following uses the **show metrics summary** command as an example. Run this command immediately after clearing metric data.
	Hostname#

Common Errors

N/A

1.4 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays the summary of existing metrics.	**show metrics define summary**
Displays the summary of existing metrics in a specified metric group.	**show metrics define summary group** *group-name*
Displays metric details.	**show metrics detail** *group-name metrics-name*
Displays the summary of all metrics.	**show metrics summary**
Displays the summary of all metrics in a specified metric group.	**show metrics summary group** *group-name*

Debugging

N/A

Configuring Security

1. Configuring ACL
2. Configuring ARP Check
3. Configuring Gateway-targeted ARP Spoofing Prevention
4. Configuring Global IP-MAC Address Binding
5. Configuring IP Source Guard
6. Configuring CPP
7. Configuring NFPP
8. Configuring Password Policies
9. Configuring SSH

1 Configuring ACL

1.1 Overview

An access control list (ACL) permits or discards data packets on a network device interface by defining access control entries (ACEs).

ACLs are classified by function into two types:

- Security ACLs: Used to control data flows that are allowed to pass through a network device.
- Quality of service (QoS) ACLs: Used to classify and process data flows by priority.

ACLs are configured for a lot of reasons. Major reasons include:

- Network access control:To ensure network security, rules are defined to limit access of users to some services (for example, only access to the WWW and email services is permitted, and access to other services such as Telnet is prohibited), or to allow users to access services in a specified period of time, or to allow only specified hosts to access the network.
- QoS: QoS ACLs are used to preferentially classify and process important data flows. For details about the use of QoS ALCs, see the configuration manual related to QoS.

1.2 Applications

N/A

1.3 Features

Basic Concepts

↘ ACL

ACLs include basic ACLs and dynamic ACLs.

You can select basic or dynamic ACLs as required. In most scenarios, basic ACLs can meet security requirements. However, an attacker may access the network by using a forged source address through software. Before a user accesses the network, a dynamic ACL requires the user to pass identity authentication, which makes it hard for hackers to attack the network. Therefore, the dynamic ACL can be used in some sensitive areas to ensure network security.

IP address spoofing is an inherent problem of all ACLs, including dynamic ACLs. Hackers may use forged IP addresses to access the network during the validity period of authenticated user identities. Two methods are available to resolve this problem. One is to set the idle time of user access to a smaller value, which increases the difficulty in intruding networks. The other is to encrypt network data using the IPSec protocol, which ensures that all data is encrypted when arriving at a device.

ACLs are generally configured on the following network devices:

- Devices between the internal network and the external network (such as the Internet)
- Devices on the border of two network segments
- Devices connected to controlled ports

ACL statements must be executed in strict compliance with their sequence in the ACL. Comparison starts from the first statement. Once the header of a data packet matches a statement in the ACL, the subsequent statements are ignored and no longer checked.

↘ Input/Output ACLs, Filtering Field Template, and Rules

When receiving a packet on an interface, the device checks whether the packet matches any access control entry (ACE) in the input ACL of this interface. Before sending a packet through an interface, the device checks whether the packet matches any ACE in the output ACL of this interface.

When different filtering rules are defined, all or only some rules may be applied simultaneously. If a packet matches an ACE, this packet is processed according to the action policy (permit or deny) defined in this ACE. ACEs in an ACL identify Ethernet packets based on the following fields in the Ethernet packets:

Layer 2 fields:

- 48-bit source MAC address (containing all 48 bits)
- 48-bit destination MAC address (containing all 48 bits)
- 16-bit Layer 2 type field

Layer 3 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 fields:

- Either a TCP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.
- Either a UDP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.

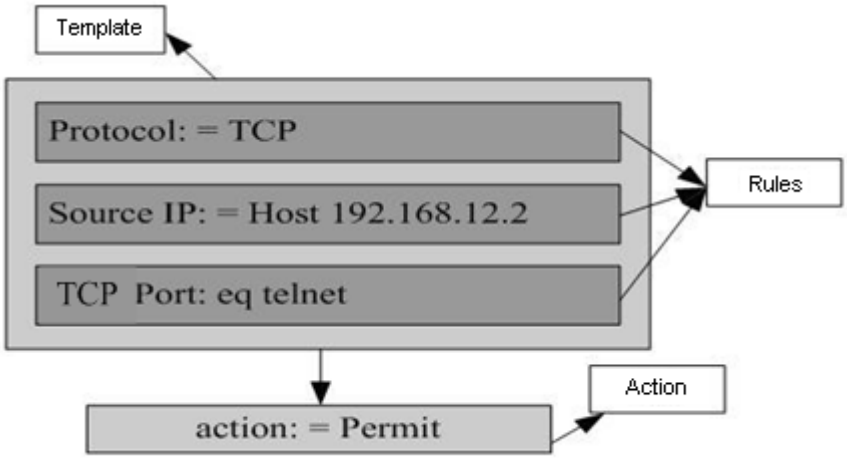
Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field in each packet; when another ACE is generated, packets are identified and classified based on the source IP address field and UDP source port field in each packet. The two ACEs use different filtering field templates.

Rules refer to values of fields in the filtering field template of an ACE. For example, the content of an ACE is as follows:

```
permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filtering field template is a combination of the following fields:source IP address field, IP protocol field, and TCP destination port field. The corresponding values (rules) are as follows:source IP address = Host 192.168.12.2; IP protocol = TCP; TCP destination port = Telnet.

Figure 1-1 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



- A filtering field template can be a combination of Layer 3 and Layer 4 fields, or a combination of multiple Layer 2 fields. The filtering field template of a standard or an extended ACL, however, cannot be a combination of Layer 2 and Layer 3 fields, a combination of Layer 2 and Layer 4 fields, or a combination of Layer 2, Layer 3, and Layer 4 fields. To use a combination of Layer 2, Layer 3, and Layer 4 fields, you can use the expert ACLs.
- An SVI associated with ACLs in the outgoing direction supports the IP standard, IP extended, MAC extended, and expert ACLs.
- If a MAC extended or expert ACL is configured to match the destination MAC address and is applied to the outbound direction of an SVI, the ACEs containing the destination MAC address can be configured but cannot take effect. If an ACE in an IP standard ACL, IP extended ACL, or expert ACL is configured to match the destination IP address, and the destination IP address is not in the subnet IP address range of the associated SVI, the ACE cannot take effect. For example, the address of VLAN 1 is 192.168.64.1 255.255.255.0, and an IP extended ACL is created and contains the ACE **deny udp any 192.168.65.1 0.0.0.255 eq 255**. If the ACL is applied to the outbound interface of VLAN 1, the ACL cannot take effect because the destination IP address is not within the subnet IP address range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, the ACL can take effect because the destination IP address is within the subnet IP address range of VLAN 1.
- The ACL applied to the outbound direction of a physical interface or aggregate interface can match only well-known packets (unicast and multicast) but not unknown unicast packets. That is, such an ACL is ineffective for the unknown or broadcast packets.
- When the ingress ACL, 802.1X, global IP-MAC binding, port security, and IP source guard are all configured, the ACEs with permit statements and default deny statement do not take effect but other ACEs with deny statements take effect.
- When both the ingress ACL and QoS ACL are configured, the ACEs with permit statements do not take effect, but ACEs with deny statements except the default deny statement take effect. The QoS ACL takes precedence over the ACL that contains the default deny statement.

An ACE is added to the ACL that has been applied to the inbound direction of multiple SVIs, and the device is restarted after the configuration is saved. In this case, the ACL may fail to be configured on several SVIs due to limitation on the hardware.

If ACEs of an ACL (IP ACL or expert extended ACL) are configured to match non-Layer 2 fields (such as SIP and DIP), the ACL does not take effect on tagged MPLS packets.

Overview

Feature	Description
IP ACL	Control incoming or outgoing IPv4 packets of a device based on the Layer 3 or Layer 4 information in the IPv4 packet header.
MAC Extended ACL	Control incoming or outgoing Layer 2 packets of a device based on the Layer 2 information in the Ethernet packet header.
Expert Extended ACL	Combine the IP ACL and MAC extended ACL into an expert extended ACL, which controls (permits or denies) incoming or outgoing packets of a device using the same rule based on the Layer 2, Layer 3, and Layer 4 information in the packet header.
IPv6 ACL	Control incoming or outgoing IPv6 packets of a device based on the Layer 3 or Layer 4 information in the IPv6 packet header.
Security Channel	Allow packets to bypass the check of access control applications, such as DOT1X and Web authentication, to meet requirements of some special scenarios.

1.3.1 IP ACL

The IP ACL implements refined control on incoming and outgoing IPv4 packets of a device. You can permit or deny the entry of specific IPv4 packets to a network according to actual requirements to control access of IP users to network resources.

Working Principle

Define a series of IP access rules in the IP ACL, and then apply the IP ACL either in the incoming or outgoing direction of an interface or globally. The device checks whether the incoming or outgoing IPv4 packets match the rules and accordingly forwards or blocks these packets.

To configure an IP ACL, you must specify a unique name or ID for the ACL of a protocol so that the protocol can uniquely identify each ACL. The following table lists the protocols that can use IDs to identify ACLs and the range of IDs.

Protocol	ID Range
Standard IP	1–99, 1300–1999
Extended IP	100–199, 2000–2699

Basic ACLs include the standard IP ACLs and extended IP ACLs. Typical rules defined in an ACL contain the following matching fields:

- Source IP address
- Destination IP address
- IP protocol number

- Layer 4 source port ID or ICMP type
- Layer 4 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 ACL rule is ineffective for ICPM packets whose ICPM type is 3. If the ICPM code of ICMP packets to be matched is configured in an ACL rule, the ACL matching result of incoming ICMP packets of a device whose ICPM 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    eqtelnetany
```

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** { **extended** | **standard** } { *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** } { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } [**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** } { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } [**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* { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } { *destination-ip-address destination-ip-wildcard* | **any** | **host** *destination-ip-address* } [**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* { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } { *destination-ip-address destination-ip-wildcard* | **any** | **host** *destination-ip-address* } [**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 or outgoing IP packets of the device.

Run the **ip access-group** { *acl-id* | *acl-name* } { **in** | **out** } command in interface configuration mode to apply a standard or an extended IP ACL to a specified interface.

1.3.2 MAC Extended ACL

The MAC extended ACL implements refined control on incoming and outgoing packets based on the Layer 2 header of packets. You can permit or deny the entry of specific Layer 2 packets to a network, thus protecting network resources against attacks or control users' access to network resources.

Working Principle

Define a series of MAC access rules in the MAC extended ACL, and then apply the ACL to the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure a 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 a 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 created MAC extended ACL contains an implicit deny statement for all Layer 2 packets. The implicit deny statement is invisible to users, but the interface where the ACL with this statement is applied drops all Layer 2 packets. Therefore, to allow specific Layer 2 packets to arrive at or go out of a device, configure matching rules in the ACL.

Matching rules can be configured in the following ways.

Regardless of a named or numbered MAC extended ACL, use the **[sn] { deny | permit } { source-mac-address source-mac-mask | any | host source-mac-address } { destination-mac-address destination-mac-mask | any | host destination-mac-address } [ethernet-type] [cos [cos] [inner cos]]** command in MAC extended ACL mode to configure a matching rule for the ACL.

For the numbered MAC extended ACL, in addition to using the preceding command, you can also use the **access-list acl-id { deny | permit } {source-mac-addresssource-mac-mask | any | host source-mac-address } {destination-mac-addressdestination-mac-mask | any | host destination-mac-address }[ethernet-type] [cos [cos] [inner cos]]** command in configuration mode to configure a matching rule for the MAC extended ACL.

↘ 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 or outgoing Layer 2 packets of a device.

Run the **mac access-group** { *acl-id* | *acl-name* } { **in** | **out** } command in interface configuration mode to apply a MAC extended ACL to a specified interface.

1.3.3 Expert Extended ACL

You can create an expert extended ACL to match the Layer 2 and Layer 3 information in packets using the same rule. The expert extended ACL can be treated as a combination and enhancement of the IP ACL and the MAC extended ACL because the expert extended ACL can contain ACEs in both the IP ACL and the MAC extended ACL. In addition, the VLAN ID can be specified in the expert extended ACL to filter packets.

Working Principle

Define a series of access rules in the expert extended ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an expert extended ACL, you must specify a unique name or ID for this ACL so that the protocol can uniquely identify each ACL. The following table lists the ID range of the expert extended ACL.

Protocol	ID Range
Expert extended ACL	2700–2899

When an expert extended ACL is created, defined rules can be applied to all packets. The device determines whether to forward or block packets by checking whether packets match these rules.

Typical rules defined in an expert extended ACL include:

- All information in the basic ACL and MAC extended ACL
- VLAN ID

The expert extended ACL (ID range: 2700–2899) is a combination of the basic ACL and MAC extended ACL, and can filter packets based on the VLAN ID.

For an individual expert extended ACL, multiple independent statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL.

If rules in an expert extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the expert extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

Implicit "Deny All Traffic" Rule Statement

At the end of every expert extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 2700permit 0x0806 any any any any any
```

This ACL permits only ARP packets whose Ethernet type is 0x0806, and denies all other types of packets. This is because the following statement exists at the end of this ACL: **access-list 2700 deny any any any any**.

Related Configuration

Configuring an Expert Extended ACL

By default, no expert extended ACL is configured on a device.

Run the **expert access-list extended** { *acl-id* | *acl-name* } command in global configuration mode to create an expert extended ACL and enter expert extended ACL mode.

Configuring Matching Rules for an Expert Extended ACL

By default, a created expert extended ACL contains an implicit deny statement for all Layer 2 packets. The implicit deny statement is invisible to users, but the interface where the ACL with this statement is applied drops all Layer 2 packets. Therefore, to allow specific Layer 2 packets to arrive at or go out of a device, configure matching rules in the ACL.

Matching rules can be configured in the following ways.

- Regardless of a named or numbered expert extended ACL, use the [*sn*] { **deny** | **permit** } [*protocol* | [*ethernet-type*] [**cos** [*cos*] [**inner** *cos*]]] [**VID** [*vid*] [**inner** *vid*]] { *source source-wildcard* | **any** | **host** *source* } { *source-mac-address source-mac-mask* | **any** | **host** *source-mac-address* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] { *destination destination-wildcard* | **any** | **host** *destination* } { **any** | **host** *destination-mac-address* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] command in expert extended ACL mode to configure a matching rule for the ACL.
- For the numbered MAC expert extended ACL, in addition to using the preceding command, you can also use the **access-list** *acl-id* { **deny** | **permit** } [*protocol* | [*ethernet-type*] [**cos** [*cos*] [**inner** *cos*]]] [**VID** [*vid*] [**inner** *vid*]] { *source source-wildcard* | **any** | **host** *source* } { *source-mac-address source-mac-mask* | **any** |

host *source-mac-address* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] { *destination destination-wildcard* | **any** | **host** *destination* } { **any** | **host** *destination-mac-address* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*] command in configuration mode to configure a matching rule for the expert extended ACL.

Applying an Expert Extended ACL

By default, the expert extended ACL is not applied to any interface, that is, the created expert extended ACL does not filter incoming or outgoing Layer 2 or Layer 3 packets of a device.

Run the **expert access-group** { ***acl-id*** | ***acl-name*** } { **in** | **out** } command in interface configuration mode to apply an expert extended ACL to a specified interface.

1.3.4 IPv6 ACL

The IPv6 ACL implements refined control on incoming and outgoing IPv6 packets of a device. You can permit or deny the entry of specific IPv6 packets to a network according to actual requirements to control access of IPv6 users to network resources.

Working Principle

Define a series of IPv6 access rules in the IPv6 ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing IPv6 packets match the rules and accordingly forwards or blocks these packets.

To configure an IPv6 ACL, you must specify a unique name for this ACL.

- Unlike the IP ACL, MAC extended ACL, and expert extended ACL, you can specify only a name but not an ID for the IPv6 ACL created.
- Only one IP ACL, or one MAC extended ACL, or one expert extended ACL can be applied to the incoming or outgoing direction of an interface. Besides, one more IPv6 ACL can be applied.

Implicit "Deny All Traffic" Rule Statement

At the end of every IPv6 ACL is an implicit "deny all IPv6 traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
ipv6 access-list ipv6_acl
 10 permit ipv6 host 200::1 any
```

This ACL permits only IPv6 packets from the source host 200::1, and denies IPv6 packets from all other hosts. This is because the following statement exists at the end of this ACL: deny ipv6 any any.

- Although the IPv6 ACL contains the implicit "deny all IPv6 traffic" rule statement by default, it does not filter ND packets.

Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When

determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and permits all IPv6 traffic, all subsequent statements will not be checked.

For example:

```
ipv6 access-list ipv6_acl
10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

As the first rule statement permits all IPv6 packets, all IPv6 packets sent from the host 200::1 does not match the subsequent deny rule with the serial number of 20, and therefore will not be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

Configuring an IPv6 ACL

By default, no IPv6 ACL is configured on a device.

Run the **ipv6 access-list** *acl-name* command in global configuration mode to create an IPv6 ACL and enter IPv6 ACL mode.

Adding ACEs to an IPv6 ACL

By default, a created IPv6 ACL contains an implicit deny statement for all IPv6 packets. The implicit deny statement is invisible to users, but the interface where the ACL with this statement is applied drops all IPv6 packets. Therefore, to allow specific IPv6 packets to arrive at or go out of a device, configure matching rules in the ACL.

Use the **[sn] { deny | permit } protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address } [lt port | eq port | gt port | neq port | range lower upper] { destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address } [lt port | eq port | gt port | neq port | range lower upper] [flow-label flow-label] [time-range time-range-name]** command in IPv6 ACL mode to configure a matching rule for the IPv6 ACL.

Applying an IPv6 ACL

By default, the IPv6 ACL is not applied to any interface, that is, the IPv6 ACL does not filter incoming or outgoing IPv6 packets of a device.

Run the **ipv6 traffic-filter** *acl-name* { **in** | **out** } command in interface configuration mode to apply an IPv6 ACL to a specified interface.

1.3.5 Security Channel

In some application scenarios, packets meeting some characteristics may need to bypass the checks of access control applications. For example, before DOT1X authentication, users are allowed to log in to a specified website to download the DOT1X authentication client. The security channel can be used for this purpose. When

the security channel configuration command is executed to apply a secure ACL globally or to an interface or VXLAN, this ACL becomes a security channel.

Working Principle

The security channel is also an ACL, and can be configured globally or for a specified interface or VXLAN. When arriving at an interface, packets are check on the security channel. If meeting the matching conditions of the security channel, packets directly enters a switch without undergoing the access control, such as port security, Web authentication, 802.1x, and IP+MAC binding check. A globally applied security channel takes effect on all interfaces except exclusive interfaces.

- The deny ACEs in an ACL that is applied to a security channel do not take effect. In addition, this ACL does not contain an implicit "deny all traffic" rule statement at the end of the ACL. If packets do not meet matching conditions of the security channel, they are checked according to the access control rules in compliance with the relevant process.
- You can configure up to eight exclusive interfaces for the global security channel. In addition, you cannot configure interface-based security channel on these exclusive interfaces.
- If a security channel is applied to an interface while a global security channel exists, this global security channel does not take effect on this interface.
- If both port-based migratable authentication mode and security channel are applied to an interface, the security channel does not take effect.
- An IPv6 ACL cannot be configured as a security channel.
- Only switches support the security channel.

Related Configuration

Configuring an ACL

Before configuring the security channel, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, or expert extended ACL.

Configuring a VXLAN Security Channel

By default, no VXLAN security channel is configured on a device.

Run the **security access-group** { *acl-id* | *acl-name* } command in VXLAN configuration mode to configure a VXLAN security channel.

Configuring a Global Security Channel

By default, no global security channel is configured on a device.

Run the **security global access-group** { *acl-id* | *acl-name* } command in global configuration mode to configure a global security channel.

Configuring an Exclusive Interface for the Global Security Channel

By default, no exclusive interface is configured for the global security channel on a device.

Run the **security uplink enable** command in interface configuration mode to configure a specified interface as the exclusive interface of the global security channel.

1.4 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.
	ip access-list resequence	Resequences an 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 time-range	Adds a permit ACE to an extended IP ACL.
	deny host any host any time-range	Adds a deny ACE to an extended IP ACL.
	ip access-list resequence	Rearranges sequence numbers of ACEs for an IP standard or extended ACL.
	ip access-group in out	Applies a standard or an extended IP ACL.
Configuring a MAC Extended ACL	⚠ (Optional) It is used to filter Layer 2 packets.	
	mac access-list extended	Configures a MAC extended ACL.
	mac access-list resequence	Resequences a MAC extended ACL
	permit any host any host cos inner time-range	Adds a permit ACE to a MAC extended ACL.
	deny any host any host cos inner time-range	Adds a deny ACE to a MAC extended ACL.
	mac access-list resequence	Rearranges sequence numbers of ACEs for an MAC extended ACL.
	mac access-group in out	Applies a MAC extended ACL.
Configuring an Expert Extended ACL	⚠ (Optional) It is used to filter Layer 2 and Layer 3 packets.	
	expert access-list extended	Configures an expert extended ACL.
	expert access-list resequence	Resequences an expert extended ACL
	permit cos inner VID inner host any host any host any host any time-range	Adds a permit ACE to an expert extended ACL.
	deny cos inner VID inner host any host any host any host any time-range	Adds a deny ACE to an expert extended ACL.
	expert access-list resequence	Rearranges sequence numbers of ACEs for an expert extended ACL.
	expert access-group in out	Applies an expert extended ACL.

Configuration Item	Description and Command	
Configuring an IPv6 Extended ACL	⚠ (Optional) It is used to filter IPv6 packets.	
	ipv6 access-list	Configures an IPv6 ACL.
	ipv6 access-list resequence	Resequences an IPv6 ACL.
	permit host any host any flow-label time-range	Adds a permit ACE to an IPv6 ACL.
	deny host any host any flow-label time-range	Adds a deny ACE to an IPv6 ACL.
	ipv6 access-list resequence	Rearranges sequence numbers of ACEs for an IPv6 ACL.
	ipv6 traffic-filter in out	Applies an IPv6 ACL.
Configuring a Security Channel	⚠ (Optional) It is used to enable packets meeting some characteristics to bypass the checks of access control applications, such as the DOT1X and Web authentication.	
	security access-group	Enables the security channel in interface configuration mode.
	security global access-group	Enables the security channel in global configuration mode.
	security uplink enable	Configures an interface as the exclusive interface of the global security channel in interface configuration mode.
Configuring the Time Range-Based ACEs	⚠ (Optional) It is used to configure ACE based on time range.	
	time-range	Configures rules based on the time range.
Configuring Comments for ACLs	⚠ (Optional) It is used to configure comments for an ACL or ACE so that users can easily identify the functions of the ACL or ACE.	
	list-remark	Configures a comment for an ACL in ACL configuration mode.
	access-list list-remark	Configures a comment for an ACL in global configuration mode.
	access-list remark	Configures a comment for an ACE in ACL configuration mode.
	remark	Configures a comment for an ACE in ACL configuration mode.

1.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface to control all incoming and outgoing IPv4 packets of this interface. You can permit or deny the entry of specific IPv4 packets to a network to control access of IP users to network resources.

Notes

N/A

Configuration Steps

Configuring an IP ACL

- (Mandatory) Configure an IP ACL if you want to control access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IP ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an IP ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv4 packets of the device are denied by default.

Rearranging Sequence Numbers of ACEs

- Optional. Rearrange sequence numbers of ACEs in an ACL to regularize them.

Applying an IP ACL

- Mandatory. You must apply an IP ACL to a specified device interface so that the IP ACL can take effect.
- Based on user distribution, you can apply an IP extended ACL to a specified interface of an access, aggregation, or core device.
- Mandatory. You must apply an IP ACL to a specified device interface so that the IP ACL can 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** { **extended** | **standard** } { *acl-id* | *acl-name* }
Parameter	**extended**: Indicates that an extended IP ACL is created.

Description	**standard**: Indicates that a standard IP ACL is created. *acl-id*: Indicates the ID that uniquely identifies a standard or extended IP ACL. If this option is configured, a numbered ACL is created. If a standard IP ACL is created, the value range of *acl-id* is 1–99 and 1300–1999. If an extended IP ACL is created, the value range of *acl-id* is 100–199 and 2000–2699. *acl-name*: Indicates the name of a standard or an extended IP ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".
Command Mode	Global Configuration mode
Usage Guide	Run this command to configure a standard or an extended IP ACL and enter standard or extended IP ACL configuration mode. If you want to control access of users to network resources by checking the source IP address of each packet, configure a standard IP ACL. If you want to control access of users to network resources by checking the source or destination IP address, protocol number, and TCP/UDP source or destination port, configure an extended IP ACL.

↘ Adding ACEs to an IP ACL

- Add ACEs to a standard IP ACL.

Use either of the following methods to add ACEs to a standard IP ACL:

Command	[*sn*] { **deny** | **permit** } { | **deny** } {**host** *source* | **any** | *source source-wildcard* | **any** | **host** *source* } [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *source-ip-address source-ip-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-ip-address*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs in standard IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } [**time-range** *time-range-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 1300–1999. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *source-ip-address source-ip-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-ip-address*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in global configuration mode. It cannot be used to add ACEs to a named IP ACL.

- Add ACEs to an extended IP ACL.

Use either of the following methods to add ACEs to an extended IP ACL:

Command	[*sn*] { **deny** | **permit** } *protocol* {*source source-wildcard* | **any** | **host** *source* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] { *destination destination-wildcard* | **any** | **host** *destination* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *source-ip-address source-ip-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source-ip-address*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *destination-ip-address destination-ip-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered.

	host *destination-ip-address:* 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. **any**: Indicates that IP packets sent to or from any host are filtered. **lt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is smaller than the port number specified by this parameter. **eq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is equal to the port number specified by this parameter. **gt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is larger than the port number specified by this parameter. **neq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is not equal to the port number specified by this parameter. **range** *lower upper*: Indicates that the TCP or UDP packet containing a Layer 4 destination port number in the specified range is to be matched. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs in extended IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **deny** | **permit** } *protocol* {*source source-wildcard* | **any** | **host** *source* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] { *destination destination-wildcard* | **any** | **host** *destination* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] [**time-range** *time-range*
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 2000–1999. *sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *source-ip-address source-ip-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source-ip-address*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *destination-ip-address destination-ip-wildcard:* Indicates that IP packets sent to hosts in a specified

	IP network segment are filtered. **host** *destination-ip-address:* 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. **any**: Indicates that IP packets sent to or from any host are filtered. **lt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is smaller than the port number specified by this parameter. **eq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is equal to the port number specified by this parameter. **gt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is larger than the port number specified by this parameter. **neq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is not equal to the port number specified by this parameter. **range** *lower upper*: Indicates that the TCP or UDP packet containing a Layer 4 destination port number in the specified range is to be matched. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in extended IP ACL configuration mode. It cannot be used to add ACEs to a named extended IP ACL.

Rearranging Sequence Numbers of ACEs

Command	**ip access-list resequence** { *acl-id* | *acl-name* } *start-sn inc-sn*
Parameter Description	*acl-id*: Indicates the numbered IP standard or extended ACL. *acl-name*: Indicates the named IP standard or extended ACL. *start-sn*: Indicates that the start value of the sequence number is configured. *inc-sn*: Indicates that the sequence number increment is configured.
Command Mode	Global configuration mode
Usage Guide	In practice, ACEs may be added to or deleted from an IP standard or extended ACL several times. After a given period of time, the sequence numbers are irregular. You can use this command to rearrange sequence numbers of ACEs to regularize them.

Applying an IP ACL

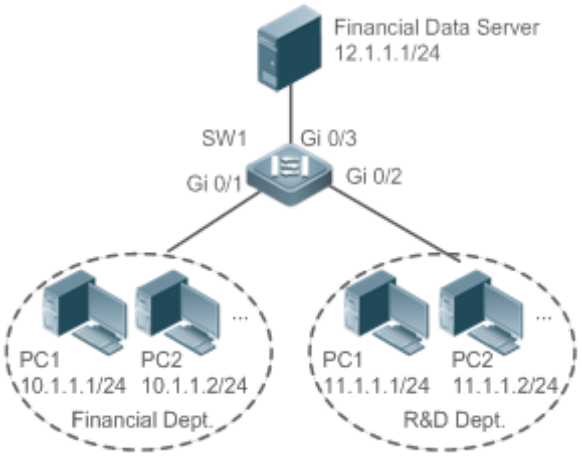
Command	**ip access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }
Parameter Description	● *acl-id*: Indicates that a numbered standard or extended IP ACL will be applied to the interface. ● *acl-name*: Indicates that a named standard or extended IP ACL will be applied to the interface. ● **in**: Indicates that this ACL controls incoming IP packets of the interface. **out**: Indicates that this ACL controls outgoing IP packets of the interface.

Command Mode	Interface configuration mode
Usage Guide	This command makes an IP ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an IP ACL to Prohibit Departments Except the Financial Department from Accessing the Financial Data Server

Scenario Figure 1-2	
Configuration Steps	● Configure an IP ACL. ● Add ACEs to the IP ACL. ● Apply the IP ACL to the outgoing direction of the interface connecting the financial data server.
AP	sw1(config)#ip access-list standard 1 sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
Verification	● On a PC of the R&D department, ping the financial data server. Verify that the ping operation fails. ● On a PC of the financial department, ping the financial data server. Verify that the ping operation succeeds.
AP	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 out Applied On interface GigabitEthernet 0/3

1.4.2 Configuring a MAC Extended ACL

Configuration Effect

Configure and apply a MAC extended ACL to an interface to control all incoming and outgoing IPv4 packets of this interface. You can permit or deny the entry of specific Layer 2 packets to a network to control access of users to network resources based on Layer 2 packets.

Notes

N/A

Configuration Steps

↘ Configuring a MAC Extended ACL

- (Mandatory) Configure a MAC extended ACL if you want to control users' access to network resources based on the Layer 2 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.

↘ Resequencing a MAC Extended ACL

- (Optional) Resequence a MAC extended access list.

↘ Rearranging Sequence Numbers of ACEs

- (Optional) Rearrange sequence numbers of ACEs in an ACL to regularize them.a MAC

↘ Applying a MAC extended ACL

- (Mandatory) Apply a MAC extended ACL to a specified interface if you want this ACL take effect.

- You can apply a 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 a 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, a 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 a 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 Layer 2 packets meeting some specified characteristics to check whether the MAC extended ACL takes effect. Typically, prepare two PCs, construct and send Layer 2 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 a MAC Extended ACL

Command	**mac access-list extended** { *acl-id* | *acl-name* }
Parameter Description	*acl-id*: Indicates the ID that uniquely identifies a MAC extended ACL. If this option is configured, a numbered ACL is created. The value range of *acl-id* is 700–799. *acl-name*: Indicates the name of a 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".
Command Mode	Global Configuration mode
Usage Guide	Run this command to configure a MAC extended ACL and enter MAC extended ACL configuration mode. You can configure a MAC extended ACL to control users' access to network resources by checking the Layer 2 information of Ethernet packets.

↘ a MACa MACa MACAdding ACEs to a MAC Extended ACL

Use either of the following methods to add ACEs to a MAC extended ACL:

- Add ACEs in MAC extended ACL configuration mode.

Command	[*sn*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** | **host** *source-mac-address* } { *destination-mac-address destination-mac-mask* | **any** | **host** *destination-mac-address* } [*ethernet-type*] [**cos** [*cos*] [**inner** *cos*]]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus

	the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **any**: Indicates that Layer 2 packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *ethernet-type*: Indicates that Layer 2 packets of the specified Ethernet type are filtered. **cos** *cos*: Indicates that Layer 2 packets with the specified class of service (cos) field in the outer tag are filtered. **inner** *cos*: Indicates that Layer 2 packets with the specified cos field in the inner tag are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	MAC extended ACL configuration mode
Usage Guide	Run this command to add ACEs in MAC extended ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to a MAC extended ACL in global configuration mode.

Command	**access-list** *acl-id* { **permit** | **deny** } { *source-mac-address source-mac-wildcard* | **any** | **host** *source-mac-address* } { *destination-mac-address destination-mac-wildcard* | **any** | **host** *destination-mac-address* } [*ethernet-type*] [**cos** [*out*] [**inner** *in*]] [**time-range** *time-range-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 700–799. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *ethernet-type*: Indicates that Layer 2 packets of the specified Ethernet type are filtered. **cos** *cos*: Indicates that Layer 2 packets with the specified cos field in the outer tag are filtered. **inner** *cos*: Indicates that Layer 2 packets with the specified cos field in the inner tag are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered MAC extended ACL in global configuration mode.

	It cannot be used to add ACEs to a named MAC extended ACL.

Rearranging Sequence Numbers of ACEs

Command	**mac access-list resequence** { *acl-id* | *acl-name* } *start-sn inc-sn*
Parameter Description	*acl-id*: Indicates the numbered MAC extended ACL. *acl-name*: Indicates the named MAC extended ACL. *start-sn*: Indicates that the start value of the sequence number is configured. *inc-sn*: Indicates that the sequence number increment is configured.
Command Mode	Global configuration mode
Usage Guide	In practice, ACEs may be added to or deleted from a MAC extended ACL several times. After a given period of time, the sequence numbers are irregular. You can use this command to rearrange sequence numbers of ACEs to regularize them.

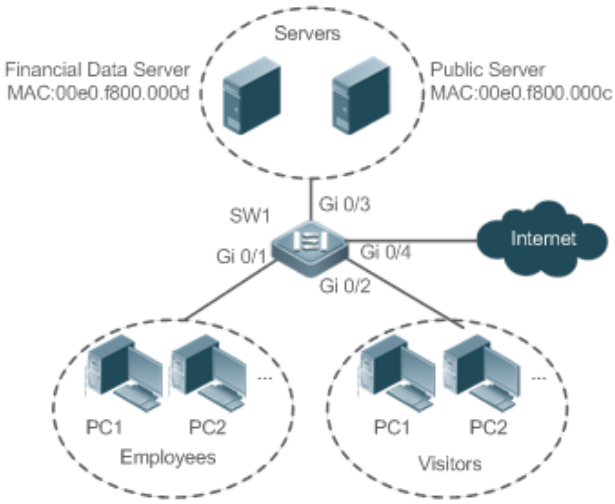
Applying a MAC Extended ACL

Command	**mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }
Parameter Description	*acl-id*: Indicates that a numbered MAC extended IP ACL will be applied to the interface. *acl-name*: Indicates that a named MAC extended IP ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming Layer 2 packets of the interface. **out**: Indicates that this ACL controls outgoing Layer 2 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes a MAC extended ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring a MAC Extended ACL to Restrict Resources Accessible by Visitors

Scenario **Figure 1-3**	

Configuration Steps	● Configure a MAC extended ACL. ● Add ACEs to the MAC extended ACL. ● Apply the MAC extended ACL to the outgoing direction of the interface connected to the visitor area so that visitors are allowed to access Internet and the public server of the company, but prohibited from accessing the financial data server of the company. That is, visitors cannot access the server with the MAC address 00e0.f800.000d.
AP	sw1(config)#mac access-list extended 700 sw1(config-mac-nacl)#deny any host 00e0.f800.000d sw1(config-mac-nacl)#pemit any any sw1(config-mac-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in
Verification	● On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ● On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
AP	sw1(config)#show access-lists mac access-list extended 700 10 deny any host 00e0.f800.000d etype-any 20 permit any any etype-any sw1(config)#show access-group mac access-group 700 in Applied On interface GigabitEthernet 0/2

1.4.3 Configuring an Expert Extended ACL

Configuration Effect

Configure and apply an expert extended ACL to an interface to control incoming and outgoing packets of the interface based on the Layer 2 and Layer 3 information, and allow or prohibit the entry of specific packets to the network. In addition, you can configure an expert extended ACL to control all Layer 2 packets based on the VLAN to permit or deny the access of users in some network segments to network resources. Generally, you can use an expert extended ACL if you want to incorporate ACEs of the IP ACL and MAC extended ACL into one ACL.

Configuration Steps

↘ **Configuring an Expert Extended ACL**

- (Mandatory) Configure an expert extended ACL if you want to control users' access to network resources based on the Layer 2 packet header, for example, the VLAN ID.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The expert extended ACL takes effect only on the local device, and does not affect other devices on the network.

Configuring Matching Rules for an Expert Extended ACL

- (Optional) An ACL can have no ACE. If no ACE is configured, no packet is allowed to enter the device.

Rearranging Sequence Numbers of ACEs

- (Optional) Rearrange sequence numbers of ACEs in an ACL to regularize them.

Applying an Expert Extended ACL

- (Mandatory) Apply an expert extended ACL to a specified interface if you want this ACL take effect.
- You can apply an expert extended ACL in the incoming or outgoing direction of a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the expert extended ACL:
- If IP-based access rules are configured in an expert extended ACL to permit or deny some IP packets, run the **ping** command to verify whether these rules take effect.
- If MAC-based access rules are configured in an expert extended ACL to permit or deny some Layer 2 packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- If VLAN ID-based access rules are configured in an expert extended ACL to permit or deny some Layer 2 packets in some network segments (e.g., to prevent communication between VLAN 1 users and VLAN 2 users), ping PCs of VLAN 2 on a PC of VLAN 1. If the ping operation fails, the rules take effect.

Related Commands

Configuring an Expert Extended ACL

Command	**expert access-list extended** { *acl-id* | *acl-name* }
Parameter Description	*acl-id*: Indicates the ID of an expert extended ACL. If this option is configured, a numbered ACL is created. The value range of *acl-id* is 2700-2899. *acl-name*: Indicates the name of an expert extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".
Command Mode	Global Configuration mode
Usage Guide	Run this command to configure an expert extended ACL and enter expert extended ACL configuration mode.

Adding ACEs to an Expert Extended ACL

Use either of the following methods to add ACEs to an expert extended ACL:

- Add ACEs in expert extended ACL configuration mode.

Command	[*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] **[** [**VID** [*out*] [**inner** *in*]]] { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } { *source-mac-address source-mac-wildcard* | **any** | **host** *source-mac-address* } { *destination-ip-address destination-ip-wildcard* | **any** | **host** *destination-ip-address* } { *destination-mac-address destination-mac-wildcard* | **any** | **host** *destination-mac-address* }] [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *ethernet-type*: Indicates that Layer 2 packets of the specified Ethernet type are filtered. **cos** *out*: Indicates that Layer 2 packets with the specified cos field in the outer tag are filtered. **cos inner** *in*: Indicates that Layer 2 packets with the specified cos field in the inner tag are filtered. **VID** *out*: Indicates that Layer 2 packets with the specified VLAN ID field in the outer tag are filtered. **VID inner** *in*: Indicates that Layer 2 packets with the specified VLAN ID field in the inner tag are filtered. *source-ip-address source-ip-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source-ip-address*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. *destination-ip-address destination-ip-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination-ip-address*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. **lt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is

	smaller than the port number specified by this parameter. **eq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is equal to the port number specified by this parameter. **gt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is larger than the port number specified by this parameter. **neq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is not equal to the port number specified by this parameter. **range** *lower upper*: Indicates that the TCP or UDP packet containing a Layer 4 destination port number in the specified range is to be matched. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Expert extended ACL configuration mode
Usage Guide	Run this command to add ACEs in expert extended ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an expert extended ACL in global configuration mode.

Command	**access-list** *acl-id* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] **[** [**VID** [*out*] [**inner** *in*]]] { *source-ip-address source-ip-wildcard* | **any** | **host** *source-ip-address* } { *source-mac-address source-mac-wildcard* | **any** | **host** *source-mac-address* } { *destination-ip-address destination-ip-wildcard* | **any** | **host** *destination-ip-address* } { *destination-mac-address destination-mac-wildcard* | **any** | **host** *destination-mac-address* }] [**time-range** *time-range-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 2700-2899. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *ethernet-type*: Indicates that Layer 2 packets of the specified Ethernet type are filtered. **cos** *out*: Indicates that Layer 2 packets with the specified cos field in the outer tag are filtered. **cos inner** *in*: Indicates that Layer 2 packets with the specified cos field in the inner tag are filtered. **VID** *out*: Indicates that Layer 2 packets with the specified VLAN ID field in the outer tag are filtered. **VID inner** *in*: Indicates that Layer 2 packets with the specified VLAN ID field in the inner tag are filtered. *source-ip-address source-ip-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source-ip-address*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered.

	destination-ip-address destination-ip-wildcard: Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination-ip-address*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. **lt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is smaller than the port number specified by this parameter. **eq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is equal to the port number specified by this parameter. **gt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is larger than the port number specified by this parameter. **neq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is not equal to the port number specified by this parameter. **range** *lower upper*: Indicates that the TCP or UDP packet containing a Layer 4 destination port number in the specified range is to be matched. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered expert extended ACL in global configuration mode. It cannot be used to add ACEs to a named expert extended ACL.

Rearranging Sequence Numbers of ACEs

Command	**expert access-list resequence** { *acl-id* | *acl-name* } *start-sn inc-sn*
Parameter Description	*acl-id*: Indicates the numbered expert extended ACL. *acl-name*: Indicates the named expert extended ACL. *start-sn*: Indicates that the start value of the sequence number is configured. *inc-sn*: Indicates that the sequence number increment is configured.
Command Mode	Global configuration mode
Usage Guide	In practice, ACEs may be added to or deleted from an expert extended ACL several times. After a given period of time, the sequence numbers are irregular. You can use this command to rearrange sequence numbers of ACEs to regularize them.

Applying an Expert Extended ACL

Command	**expert access-group** { *acl-id* | *acl-name* } { **in** | **out** }
Parameter Description	● *acl-id*: Indicates that a numbered expert extended ACL will be applied to the interface. ● *acl-name*: Indicates that a named expert extended ACL will be applied to the interface. ● **in**: Indicates that this ACL controls incoming Layer 2 packets of the interface. ● **out**: Indicates that this ACL controls outgoing Layer 2 packets of the interface.

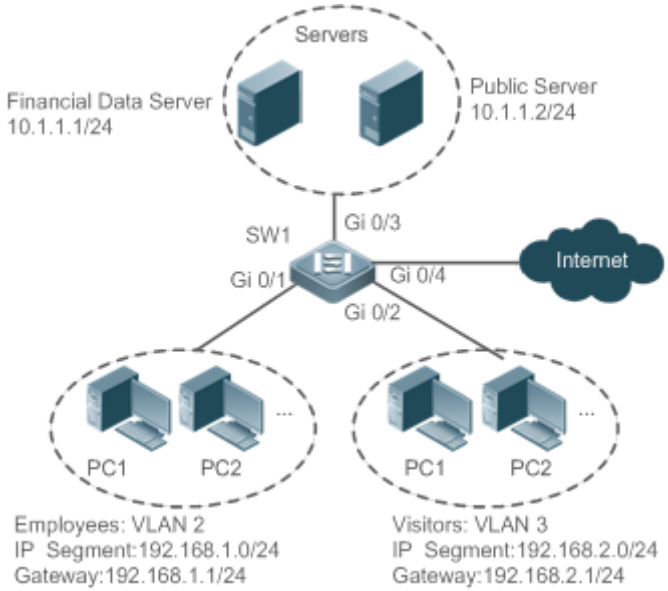
Command Mode	Interface configuration mode
Usage Guide	This command makes an expert extended ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an Expert Extended ACL to Restrict Resources Accessible by Visitors

It is required that visitors and employees cannot communicate with each other, visitors can access the public resource server but not the financial data server of the company.

Scenario Figure 1-4	
Configuration Steps	• Configure an expert extended ACL. • Add an ACE to deny packets sent from PCs in the visitor area (VLAN 3) to employee PCs in VLAN 2. • Add an ACE to prevent visitors from accessing the financial data server of the company. • Add an ACE to permit all packets. • Apply the ACL to the incoming direction of the interface of the switch that connects to the visitor area.
AP	sw1(config)#expert access-list extended 2700 sw1(config-exp-nacl)#deny ip any 192.168.1.0 0.0.0.255 any sw1(config-exp-nacl)#deny ip any host 10.1.1.1 any sw1(config-exp-nacl)#pemit any sw1(config-exp-nacl)#exit sw1(config)#int gigabitEthernet 0/2

	sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
Verification	● On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ● On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ● On a visitor's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation fails. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
AP	sw1(config)#show access-lists expert access-list extended 2700 10 deny ip any 192.168.1.0 0.0.0.255 any 20 deny ip any host 10.1.1.1 any 30 permit ip any sw1(config)#show access-group expert access-group 2700 in Applied On interface GigabitEthernet 0/2

1.4.4 Configuring an IPv6 Extended ACL

Configuration Effect

Configure and apply an IPv6 ACL to an interface to control all incoming and outgoing IPv5 packets of this interface. You can permit or deny the entry of specific IPv6 packets to a network to control access of IPv6 users to network resources.

Configuration Steps

↘ **Configuring an IPv6 ACL**

- (Mandatory) Configure an IP ACL if you want to access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

↘ **Configuring an IPv6 ACE**

- (Optional) An ACL can have no ACE. If no ACE is configured, no IPv6 packet is allowed to enter the device.

↘ **Rearranging Sequence Numbers of ACEs**

- (Optional) Rearrange sequence numbers of ACEs in an ACL to regularize them.

↘ **Applying an IPv6 ACL**

- (Mandatory) Apply an IPv6 ACL to a specified interface on a device if you want this ACL take effect.
- You can apply an IPv6 ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IPv6 ACL:
- Run the **ping** command to verify that the IPv6 ACL takes effect on the specified interface. For example, if an IPv6 ACL is configured to prohibit a host with a specified IP address or hosts in a specified IPv6 address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.
- Access network resources, for example, visit an IPv6 website, to check whether the IPv6 ACL takes effect on the specified interface.

Related Commands

Configuring an IPv6 ACL

Command	**ipv6 access-list** *acl-name*
Parameter Description	*acl-name*: Indicates the name of an IPv6 extended ACL. The name is a string of 1 to 99 characters. The ACL name cannot start with numerals (0–9), in, or out.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an IPv6 ACL and enter IPv6 configuration mode.

Adding ACEs to an IPv6 ACL

- To filter TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

Command	[*sn*] { **deny** | **permit** } *ipv6-protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] { *destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* } [**lt** *port* | **eq** *port* | **gt** *port* | **neq** *port* | **range** *lower upper*] [**flow-label** *flow-label*] [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 11 by default. You can adjust the increment using a command. **deny**: Indicates that packets are denied. **permit**: Indicates that packets are allowed. *ipv6-protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp. *source-ipv6-prefix / prefix-length:* Indicates that IP packets sent from hosts in the specified IPv6

	network segment are filtered. **host** *source-ipv6-address*: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IPv6 packets sent from any host are filtered. *destination-ipv6-prefix / prefix-length:* Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered. **host** *destination-ipv6-address*: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IPv6 packets sent to any host are filtered. **lt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is smaller than the port number specified by this parameter. **eq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is equal to the port number specified by this parameter. **gt** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is larger than the port number specified by this parameter. **neq** *port*: Indicates that the Layer 4 destination port number in TCP or UDP packets to be matched is not equal to the port number specified by this parameter. **range** *lower upper*: Indicates that the TCP or UDP packet containing a Layer 4 destination port number in the specified range is to be matched. **flow-label** *flow-label*: Indicates that IPv6 packets with the specified the flow label field in the header are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

- To filter IPv6 packets except for the TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

Command	[*sn*] { **deny** | **permit** } *ipv6-protocol* { *source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* } { *destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* } [**flow-label** *flow-label*] [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 11 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *ipv6-protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp.

	source-ipv6-prefix / prefix-length: Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered. **host** *source-ipv6-address*: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IPv6 packets sent from any host are filtered. *destination-ipv6-prefix / prefix-length:* Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered. **host** *destination-ipv6-address*: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IPv6 packets sent to any host are filtered. **flow-label** *flow-label*: Indicates that IPv6 packets with the specified the flow label field in the header are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

↘ Rearranging Sequence Numbers of ACE

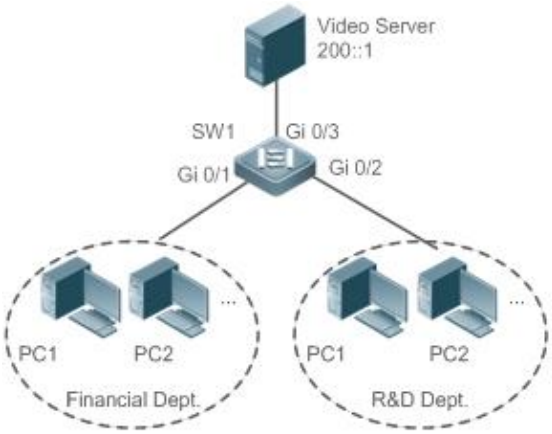
Command	**ipv6 access-list resequence** *acl-name start-sn inc-sn*
Parameter Description	*acl*-name: Indicates the IPv6 ACL name. *start-sn*: Indicates that the start value of the sequence number is configured. *inc-sn*: Indicates that the sequence number increment is configured.
Command Mode	Global configuration mode
Usage Guide	In practice, ACEs may be added to or deleted from an IPv6 extended ACL several times. After a given period of time, the sequence numbers are irregular. You can use this command to rearrange sequence numbers of ACEs to regularize them.

↘ Applying an IPv6 ACL

Command	**ipv6 traffic-filter** *acl-name* { **in** | **out** }
Parameter Description	*acl-name*: Indicates the name of an IPv6 ACL. **in**: Indicates that this ACL controls incoming IPv6 packets of the interface. **out**: Indicates that this ACL controls outgoing IPv6 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an IPv6 ACL take effect on the incoming or outgoing packets of the specified interface.

Configuration Example

↘ Configuring an IPv6 ACL to Prohibit the R&D Department from Accessing the Video Server

Scenario Figure 1-5	
Configuration Steps	● Configure an IPv6 ACL. ● Add an ACE to the IPv6 ACL to prevent access to the video server. ● Add an ACE to the IPv6 ACL to permit all IPv6 packets. ● Apply the IPv6 ACL to the incoming direction of the interface connected to the R&D department.
AP	sw1(config)#ipv6 access-list dev_deny_ipv6video sw1(config-ipv6-nacl)#deny ipv6 any host 200::1 sw1(config-ipv6-nacl)#permit ipv6 any any sw1(config-ipv6-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in
Verification	● On a PC of the R&D department, ping the video server. Verify that the ping operation fails.
AP	sw1(config)#show access-lists ipv6 access-list dev_deny_ipv6video 10 deny ipv6 any host 200::1 20 permit ipv6 any any sw1(config)#show access-group ipv6 traffic-filter dev_deny_ipv6video in Applied On interface GigabitEthernet 0/2

1.4.5 Configuring a Security Channel

Configuration Effect

The security channel function allows the device not to check the packets that match security channel rules. For example, 802.1X is enabled on an interface of the uplink device connected to a user host. A security channel can be configured to permit the user to log in to a site to download resources such as the authentication client before 802.1X authentication.Configuration Steps

↘ Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

↘ Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured for an ACL, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

↘ Configuring a Security Channel on a Specified Interface, VXLAN or Globally

- Configure a security channel on an interface if you want this security channel to take effect on the interface. Configure a VXLAN security channel if you want this security channel to take effect on VNI. Configure a global security channel if you want this security channel to take effect globally. You must configure either the interface-based security channel or the global security channel.
- You can configure a security channel on an access, an aggregate, or a core device based on the distribution of users.

↘ Configuring an Exclusive Interface for the Global Security Channel

- (Optional) Configure an interface as the exclusive interface for the global security channel if you do not want the global security channel to take effect on this interface.

↘ Configuring an Access Control Application

- (Optional) You can enable the DOT1X or Web authentication function to verify the security channel function.
- You can configure the access control function on an access, an aggregate, or a core device based on the distribution of users.

Verification

On a PC that is subject to the control of an access control application, ping the resources (devices or servers) that are allowed to bypass the check of the access control application to verify the configuration of the security channel.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring a Security Channel on an Interface

Command	**security access-group** { *acl-id* | *acl-name* }
Parameter Description	● *acl-id*: Indicates that ID of the ACL that is configured as the security channel. ● *acl-name*: Indicates that name of the ACL that is configured as the security channel.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure a specified ACL as the security channel on the specified interface.

Configuring a Global Security Channel

Command	**security global access-group** { *acl-id* | *acl-name* }
Parameter Description	● *acl-id*: Indicates that ID of the ACL that is configured as the security channel. ● *acl-name*: Indicates that name of the ACL that is configured as the security channel.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the specified ACL as the global security channel.

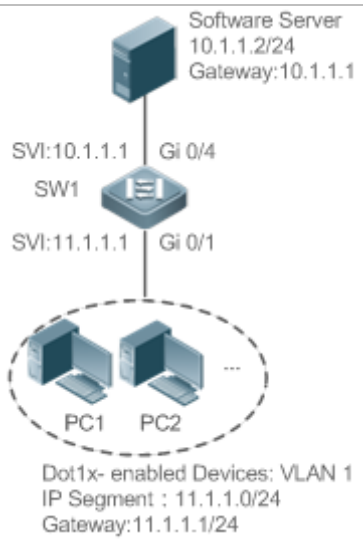
Configuring an Exclusive Interface for the Global Security Channel

Command	**security uplink enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the specified interface as the exclusive interface of the global security channel.

Configuration Example

The following configuration example describes only ACL-related configurations.

Enabling DOT1X Authentication and Configuring a Security Channel to Allow Users to Download the SU Software from the Server Before Authentication

Scenario Figure 1-7	
Configuration Steps	● Configure an expert extended ACL "exp_ext_esc". ● Add an ACE to allow forwarding packets to the destination host 10.1.1.2. ● Add an ACE to permit the DHCP packets. ● Add an ACE to permit the ARP packets. ● On the interface where DOT1X authentication is enabled, configure the ACL **exp_ext_esc** as the security channel.
SW1	sw1(config)#expert access-list extended exp_ext_esc sw1(config-exp-nacl)# permit ip any any host 10.1.1.2 any sw1(config-exp-nacl)# permit 0x0806 any any any any any sw1(config-exp-nacl)# permit tcp any any any any eq 67 sw1(config-exp-nacl)# permit tcp any any any any eq 68 sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc
Verification	● On a PC of the sales department, ping the server of the sales department. Verify that the ping operation succeeds. ● On the PCs of R&D department 1 and R&D department 2, ping the server of the sales department. Verify that the ping operations fail.
	sw1#show access-lists expert access-list extended exp_ext_esc 10 permit ip any any host 10.1.1.2 any 20 permit arp any any any any any 30 permit tcp any any any any eq 67 40 permit tcp any any any any eq 68.....

	sw1#show running-config interface gigabitEthernet 0/1 Building configuration... Current configuration : 59 bytes interface GigabitEthernet 0/1 security access-group exp_ext_esc

1.4.6 Configuring the Time Range-Based ACEs

Configuration Effect

Configure the time range-based ACEs if you want some ACEs to take effect or to become invalid in a specified period of time, for example, in some time ranges during a week.

Configuration Steps

↘ Configuring an ACL

- (Mandatory) Configure an ACL if you want ACEs to take effect in the specified time range. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

↘ Adding an ACE with the Time Range Specified

- (Mandatory) Specify the time range when adding an ACE. For details about how to configure the time range, see the configuration manual related to the time range.

↘ Applying an ACL

- (Mandatory) Apply the ACL to a specified interface if you want to make ACEs take effect in the specified time range.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

In the time range that the configured ACE takes effect or becomes invalid, run the **ping** command or construct packets matching the ACE to check whether the ACE takes effect or becomes invalid.

Related Commands

↘ Configuring an ACL

For details about the ACL configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding an ACE with the Time Range Specified

For details about the ACE configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

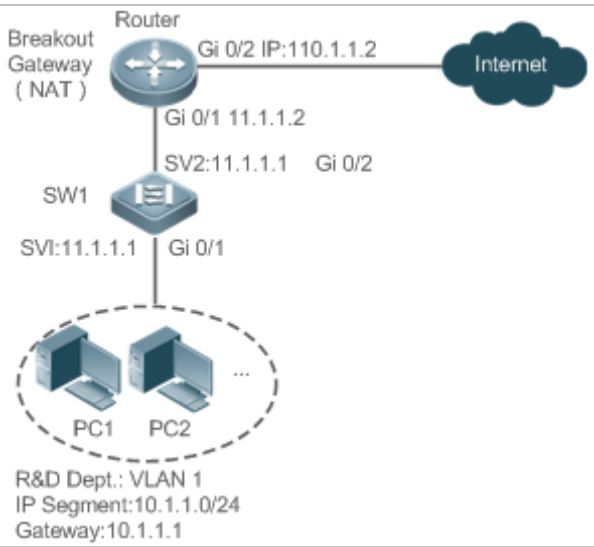
Applying an ACL

For details about the command for applying an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuration Example

The following configuration example describes only ACL-related configurations.

Adding an ACE With the Time Range Specified to Allow the R&D Department to Access the Internet Between 12:00 and 13:30 Every Day

Scenario **Figure 12-8**	
Configuration Steps	• Configure a time range named "access-internet", and add an entry of the time range between 12:00 and 13:30 every day. • Configure an IP ACL "ip_std_internet_acl". • Add an ACE to allow packets with the source IP address in the network segment 10.1.1.0/24, and associate this ACE with the time zone "access-internet". • Add an ACE to deny packets with the source IP address the network segment 10.1.1.0/24. Access to the Internet is not allowed except in the specified time range. • Add an ACE to permit all packets. • Apply the ACL to the outgoing direction of the interface connected to the breakout gateway.
AP	Hostname(config)# time-range access-internet Hostname(config-time-range)# periodic daily 12:00 to 13:30 Hostname(config-time-range)# exit

	sw1(config)# ip access-list standard ip_std_internet_acl sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255 sw1(config-std-nacl)# permit any sw1(config-std-nacl)# exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out
Verification	● Within the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website can be opened normally. ● Beyond the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website cannot be opened.
AP	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 out Applied On interface GigabitEthernet 0/2

1.4.7 Configuring Comments for ACLs

Configuration Effect

During network maintenance, if a lot of ACLs are configured without any comments, it is difficult to distinguish these ACLs later on. You can configure comments for ACLs to better understand the intended use of ACLs.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Configuring Comments for ACLs

- (Optional) Configure comments for ACLs so that it is easy to manage and understand the configured ACLs.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring Comments for ACEs

- (Optional) To facilitate understanding of a configured ACL, you can configure comments for ACEs in addition to comments for the ACL.

Verification

Run the **show access-lists** command on the device to display the comments configured for ACLs.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring a Comment for an ACL

Use either of the following two methods to configure a comment for an ACL:

Command	**list-remark** *comment*
Parameter Description	● ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACL.

Command	**access-list** *acl-id* **list-remark** *comment*
Parameter Description	● *acl-id*: Indicates the ID of an ACL. ● *comment*: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command	Global Configuration mode

Mode	
Usage Guide	Run this command to configure the comment for a specified ACL.

↘ Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

↘ Configuring Comments for ACEs

Use either of the following two methods to configure a comment for an ACE:

Command	[*sn*] **remark** *comment*
Parameter Description	● ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters. ● *sn*: Indicates the sequence number of an ACE for which a comment is required.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

Command	**access-list** *acl-id* [*sn*] **remark** *comment*
Parameter Description	● ***acl-id***: Indicates the ID of an ACL. ● ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters. ● *sn*: Indicates the sequence number of an ACE for which a comment is required.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE. If *sn* is not configured, the comment is configured for the last ACE.

1.5 Monitoring

Clearing

Description	Command
Clears the ACL packet matching counters.	**clear counters access-list** [*acl-id* | *acl-name*]
Clears statistics on denied packets.	**clear access-list counters** [*acl-id* | *acl-name*]

Displaying

Description	Command

Displays the basic ACLs.	**show access-lists** [*acl-id* | *acl-name*] [**summary**]
Displays the ACL configurations applied to an interface.	**show access-group** [**interface** *interface-name* | **wlan** *wlan*]
Displays the IP ACL configurations applied to an interface.	**show ip access-group** [**interface** *interface-name* | **wlan** *wlan-id*]
Displays the MAC extended ACL configurations applied to an interface.	**show mac access-group** [**interface** *interface-name* | **wlan** *wlan-id*]
Displays the expert extended ACL configurations applied to an interface.	**show expert access-group** [**interface** *interface-name* | **wlan** *wlan-id*]
Displays the IPv6 ACL configurations applied to an interface.	**show ipv6 traffic-filter** [**interface** *interface-name*]

Debugging

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

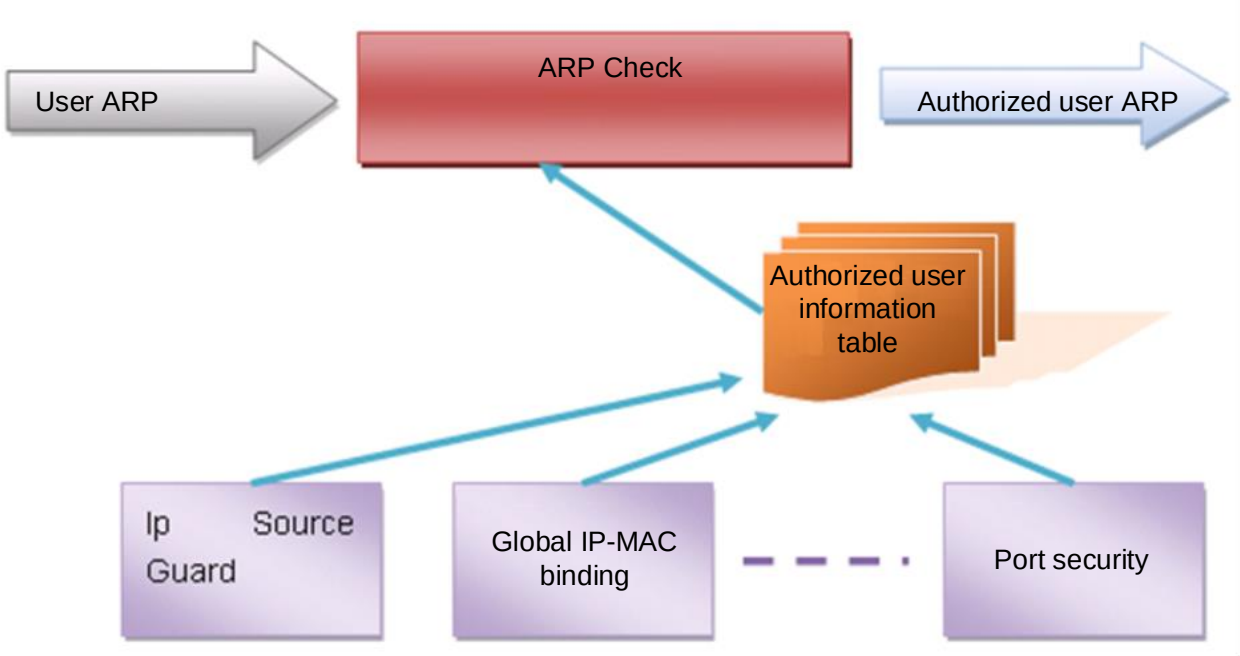
Description	Command
Debugs the ACL running process.	**debug acl acld event**
Debugs the ACL clients.	**debug acl acld client-show**
Debugs the ACLs created by all ACL clients.	**debug acl acld acl-show**

1 Configuring ARP Check

1.1 Overview

Address Resolution Protocol (ARP) Check filters all ARP packets under ports (including wired Layer 2 switching ports, Layer 2 aggregate interfaces, and Layer 2 encapsulation sub-interfaces, as well as WLAN interfaces) and discards unauthorized ARP packets, so as to effectively prevent ARP deception via networks and to promote network stability. On devices supporting ARP check, unauthorized ARP packets on networks will be ignored according to the authorized user information (IP-based or IP-MAC based) generated by security application modules such as IP source guard, global IP+MAC binding, 802.1X authentication, GSN binding, web authentication, and port security.

Figure 1-1



The above figure shows that security modules generate authorized user information (IP-based or IP-MAC based). ARP check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC>fields in all ARP packets at ports matches those in the list of authorized user information. If not, all unlisted ARP packets will be discarded.

Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

1.2 Applications

Application	Description
Filtering ARP Packets in Networks	Unauthorized users on a network launch attacks using forged ARP packets.

1.2.1 Filtering ARP Packets in Networks

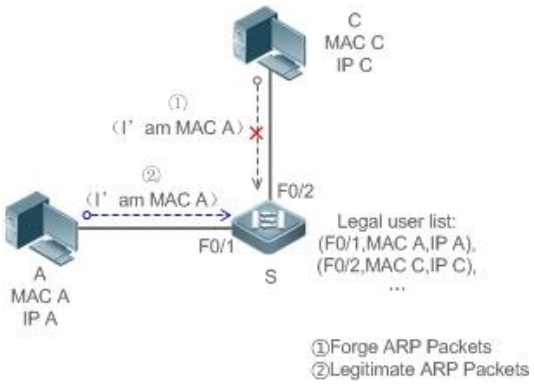
Scenario

Check ARP packets from distrusted ports and filter out ARP packets with addresses not matching the results assigned by the DHCP server.

For example, in the following figure, the ARP packets sent by DHCP clients are checked.

- The ports receiving ARP packets, the source MAC addresses of ARP packets, and the source IP addresses of ARP packets shall be consistent with the snooped DHCP-assigned records.

Figure 1-2



Remarks:	S is an access device. A and C are user PCs.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all the downlink ports on S as DHCP distrusted ports.
- Enable IP source guard and ARP check on all distrusted ports on S to realize ARP packet filtration.

1.3 Features

Basic Concepts

↘ Compatible Security Modules

Presently, the ARP check supports the following security modules.

- IP-based: IP-based mode: port security, and static configuration of IP source guard.

- IP-MAC based: IP-MAC based mode: port security, global IP+MAC binding, 802.1X authorization, IP source guard, GSN binding, and web authentication.

Two Modes of APR Check

ARP check has two modes: Enabled and Disabled. The default is Enabled.

1. Enabled Mode

Through ARP check, ARP packets are detected based on the IP/IP-MAC based binding information provided by the following modules:

- Global IP-MAC binding
- 802.1X authorization
- IP source guard
- GSN binding
- Port security
- Web authentication
- Port security, IP-MAC binding, or IP binding

⚠ If an interface is enabled with ARP check only, the device allows all ARP packets to pass through. If ARP check is enabled together with the preceding modules on the interface with no authorized user entries, all ARP packets from the interface are discarded.

⚠ When the ARP check and VRRP functions are enabled on an interface, if the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

2. Disabled Mode

ARP packets on an interface are not checked.

Overview

Feature	Description
Filtering ARP Packets	Checks the source IP and source MAC addresses of ARP packets to filter out unauthorized ARP packets.

1.3.1 Filtering ARP Packets

Enable ARP check on specified ports to realize filtration of unauthorized ARP packets.

Working Principle

A device matches the source IP and source MAC addresses of the ARP packets received at its ports with the authorized user information of the device. With successful matching, packets will be transferred, or otherwise they will be discarded.

Related Configuration

Enabling ARP Check on Ports

- By default, the ARP check is disabled on ports.
- Use the **arp-check** command to enable ARP check.
- Unless otherwise noted, this function is usually configured on the ports of access devices.

1.4 Configuration

Configuration	Description and Command	
Configuring ARP Check	⚠ (Mandatory) It is used to enable APR Check.	
	arp-check	Enables ARP check.

1.4.1 Configuring ARP Check

Configuration Effect

- Unauthorized ARP packets are filtered out.

Notes

- When ARP check is enabled, the number of policies or users of related security applications may decrease.
- ARP check cannot be configured on mirrored destination ports.
- ARP check cannot be configured on the trusted ports of DHCP Snooping.
- ARP check cannot be configured on global IP+MAC exclude ports.
- ARP check can be enabled only on wired switching ports, Layer 2 aggregate interfaces, Layer 2 encapsulation sub-interfaces, as well as WLAN interfaces. Enable ARP check for the wired in interface configuration mode, while for the wireless in WLAN security configuration mode.
- For fit APs in wired access mode, ARP check needs to be enabled in ap-config all mode.

Configuration Steps

Enabling ARP Check

- (Mandatory) The function is disabled by default. To use the ARP check function, an administrator needs to run a command to enable it.

Verification

- Use the **show running-config** command to display the system configuration.
- Use the **show wlan arp-check list** command to display filtering entries.

Related Commands

Enabling ARP Check

Command	arp-check
Parameter Description	N/A
Command	Interface configuration mode or WLAN security configuration mode
Usage Guide	Generate ARP filtration information according to the authorized user information of security application modules to filter out unauthorized ARP packets on networks. When the ARP check function is enabled in WLAN ap-config all mode, the function is enabled on wired ports of all aggregate interfaces.

Configuration Example

The following configuration example introduces only ARP check related configurations.

Enabling ARP Check on Ports

Configuration Steps	● Enable ARP check. Restricted ARP packets must conform to entries of IP source guard or global IP+MAC binding.
	Hostname# configure terminal Hostname(config)#address-bind 192.168.1.3 00d0.f800.0003 Hostname(config)#address-bind install Hostname(config)#ip source binding 00d0.f800.0002 vlan 1 192.168.1.4 interface gigabitethernet 0/1 Hostname(config)# interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# arp-check Hostname(config-if-GigabitEthernet 0/1)#ip verify source port-security Hostname(config-if-GigabitEthernet 0/1)#exit Hostname# configure terminal Hostname(config)# dot11 wlan 1 Hostname(dot11-wlan-config)# ssid TEST-SSID Hostname(dot11-wlan-config)# exit Hostname(config)#wlansec 1 Hostname(config-wlansec)# ip verify source port-security Hostname(config-wlansec)#arp-check Hostname(config-wlansec)# exit Hostname(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1
Verification	Use the **show interfaces arp-check list** command to display the effective ARP check list for interfaces.
	Hostname# show interfaces arp-check list

```
INTERFACE                 SENDER MAC         SENDER IP          POLICY SOURCE
----------------------- ---------------- ---------------- ----------------
GigabitEthernet 0/1       00d0.f800.0003     192.168.1.3        address-bind
GigabitEthernet 0/1       00d0.f800.0001     192.168.1.1        port-security
GigabitEthernet 0/1       00d0.f800.0002     192.168.1.4        DHCP snooping

Hostname# show wlan arp-check list

INTERFACE                 SENDER MAC         SENDER IP          POLICY SOURCE
----------------------- ---------------- ---------------- ----------------
Wlan 1                    0026.c79f.6e4c     172.168.131.1      DHCP snooping
```

Common Errors

- If ARP packets at a port need to be checked but APR-Check is disabled, then APR-Check will not be effective.

1.5 Monitoring

Displaying

Description	Command
Displays the effective ARP check list based on ports.	**show interfaces** [*interface-type interface-number*] **arp-checklist**
Displays the effective ARP check list based on WLAN.	**show wlan** [*wlan-id*] **arp-checklist**

1 Configuring Gateway-targeted ARP Spoofing Prevention

1.1 Overview

Gateway-targeted Address Resolution Protocol (ARP) spoofing prevention effectively prevents gateway-targeted ARP spoofing by checking on the logical port whether the source IP addresses of ARP packets (Sender IP fields of ARP packets) are the self-configured gateway IP addresses.

Protocols and Standards

RFC 826: Ethernet Address Resolution Protocol

1.2 Applications

N/A

1.3 Features

Basic Concepts

↘ ARP

ARP is a TCP/IP protocol that obtains physical addresses according to IP addresses. Its function is as follows: The host broadcasts ARP requests to all hosts on the network and receives the returned packets to determine physical addresses of the target IP addresses, and saves the IP addresses and hardware addresses in the local ARP cache, which can be directly queried in response to future requests. On the same network, all the hosts using the ARP are considered as mutually trustful to each other. Each host on the network can independently send ARP response packets; the other hosts receive the response packets and record them in the local ARP cache without detecting their authenticity. In this way, attackers can send forged ARP response packets to target hosts so that the messages sent from these hosts cannot reach the proper host or reach a wrong host, thereby causing ARP spoofing.

↘ Gateway-targeted ARP Spoofing

When User A sends an ARP packet requesting the media access control (MAC) address of a gateway, User B on the same VLAN also receives this packet, and User B can send an ARP response packet, passing off the gateway IP address as the source IP address of the packet, and User B's MAC address as the source MAC address. This is called gateway-targeted ARP spoofing. After receiving the ARP response, User A regards User B's machine as the gateway, so all the packets sent from User A to the gateway during communication will be sent to User B. In this way, User A's communications are intercepted, thereby causing ARP spoofing.

Overview

Feature	Description

Gateway-targeted ARP Spoofing Prevention	Blocks ARP spoofing packets with forged gateway address and intranet server IP addresses to ensure that users can access the Internet.

1.3.1 Gateway-targeted ARP Spoofing Prevention

Working Principle

Gateway-targeted Spoofing Prevention

Gateway-targeted ARP spoofing prevention effectively prevents ARP spoofing aimed at gateways by checking on the logical port whether the source IP addresses of ARP packets are the self-configured gateway IP addresses. If an ARP packet uses the gateway address as the source IP address, the packet will be discarded to prevent users from receiving wrong ARP response packets. If not, the packet will not be handled. In this way, only the upstream device connected to the device can send ARP packets of the gateway, and the ARP response packets sent from the other PCs which pass through the gateway are filtered by the device.

Related Configuration

Configuring Gateway-targeted Spoofing Prevention Addresses

- By default, no gateway-targeted ARP spoofing prevention address is configured.
- Run the **anti-arp-spoofing ip** command to configure the gateway-targeted ARP spoofing prevention addresses.

1.4 Configuration

Configuration	Description and Command	
Configuring Gateway-targeted Spoofing Prevention	⚠ Optional.	
	anti-arp-spoofing ip	Configures gateway-targeted ARP spoofing prevention on the logical port and specifies the gateway IP address.

1.4.1 Configuring Gateway-targeted Spoofing Prevention

Configuration Effect

Enable gateway-targeted ARP spoofing prevention.

Configuration Steps

Configuring Gateway-targeted Spoofing Prevention

- Gateway-targeted ARP spoofing prevention is mandatory. It must be enabled.

Verification

- Run the **show running-config** command to check configuration.
- Run the **show anti-arp-spoofing** command to display all data on gateway-targeted ARP spoofing prevention.

Related Commands

Configuring Gateway-targeted Spoofing Prevention

Command	**anti-arp-spoofing ip** *ipv4-address*
Parameter Description	*ipv4-address*: indicates the IPv4 address of the gateway.
Command Mode	Wireless security configuration mode
Usage Guide	

Configuration Example

N/A

1.5 Monitoring

Displaying

Description	Command
Displays all data on gateway-targeted ARP spoofing prevention.	**show anti-arp-spoofing**

1 Configuring Global IP-MAC Address Binding

1.1 Overview

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

The address bounding feature is used to verify the input packets. Note that the address binding feature takes precedence over the 802.1X authentication and port security.

1.2 Applications

N/A

Application	Description
Global IP-MAC Binding	Only hosts with the specified IP addresses can access the network, and the hosts connected to a device can move freely.

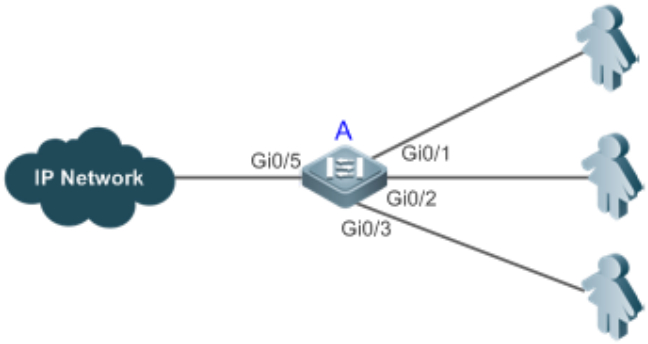
1.2.1 Global IP-MAC Binding

Scenario

The administrator assigns a fixed IP address for each host to facilitate management.

- Only hosts with the specified IP addresses can access the external network, which prevents IP address embezzlement by unauthorized hosts.
- Hosts can move freely on the same device.

Figure 1-1



Remarks	A is an access device. A user is a host configured with a static IP address. The IP network is an external IP network.

Deployment

- Manually configure the global IP-MAC binding. (Take three users as an example.)

User	MAC Address	IP Address
User 1	00d0.3232.0001	192.168.1.10
User 2	00d0.3232.0002	192.168.1.20
User 3	00d0.3232.0003	192.168.1.30

- Enable the IP-MAC binding function globally.
- Configure the uplink port (Gi0/5 port in this example) of the device as the exclude port.

1.3 Features

Basic Concepts

IPv6 Address Binding Mode

IPv6 address binding modes include Compatible, Loose, and Strict. The default mode is Strict. If IPv4-MAC binding is not configured, the IPv6 address binding mode does not take effect, and all IPv4 and IPv6 packets are allowed to pass through. If IPv4-MAC binding is configured, the IPv6 address binding mode takes effect, and the device forwards IPv4 and IPv6 packets based on the forwarding rules described in the following table.

Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the global IPv4-MAC binding are forwarded.	Packets matching the global IPv6-MAC binding are forwarded.
Loose	Packets matching the global IPv4-MAC binding are forwarded.	If IPv6+MAC address binding is configured, packets matching the IPv6-MAC binding are forwarded. If IPv6-MAC binding does not exist, all IPv6 packets are forwarded.
Compatible	Packets matching the global IPv4-MAC binding are forwarded.	If the IPv6 packets contain a MAC address matching the MAC address in the IPv4-MAC binding, the IPv6 packets are forwarded. Packets matching the global IPv6-MAC binding conditions are forwarded.

IPv4-MAC binding entries in the preceding table can be generated through global IP-MAC binding or other access security functions, such as port security and IP source guard. Similarly, IPv6-MAC binding entries can be also through global IP-MAC binding or other access security functions, such as port security and IPv6 source guard.

Exclude Port

By default, the IP-MAC binding function takes effect on all ports of the device. You can configure exclude ports so that the address binding function does not take effect on these ports. In practice, the IP-MAC bindings of the input packets on the uplink port are not fixed. Generally, the uplink port of the device is configured as the exclude port so that the packets on the uplink port are not checked for IP-MAC binding.

Overview

Feature	Description
Configuring Global IP-MAC Binding	Controls forwarding of IPv4 or IPv6 packets.
Configuring the IPv6 Address Binding Mode	Changes the IPv6 packet forwarding rules.
Configuring the Exclude Port	Disables the global address binding function on the specified port.

1.3.1 Configuring Global IP-MAC Binding

Working Principle

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

Related Configuration

↘ Configuring IP-MAC Binding

Run the **address-bind** command in global configuration mode to add or delete an IPv4-MAC binding.

↘ Enabling the IP-MAC Binding Function

Run the **address-bind install** command in global configuration mode to enable the IP-MAC binding function. By default, this function is disabled.

1.3.2 Configuring the IPv6 Address Binding Mode

Working Principle

After the global IPv4-MAC binding is configured and enabled, IPv6 packets are forwarded based on the IPv6 address binding mode. IPv6 binding modes include Compatible, Loose, and Strict.

Related Configuration

↘ Configuring the IPv6 Address Binding Mode

By default, the IPv6 address binding mode is Strict.

Run the **address-bind ipv6-mode** command to specify an IPv6 address binding mode.

1.3.3 Configuring the Exclude Port

Working Principle

Configure an exclude port so that the address binding function does not take effect on this port.

Related Configuration

↘ Configuring the Exclude Port

Run the **address-bind uplink** command to configure an exclude port. By default, no port is the exclude port.

1.4 Configuration

Configuration	Description and Command	
Configuring Global IP-MAC Binding	⚠ (Mandatory) It is used to configure and enable address binding.	
	address-bind	Configures global IP-MAC binding.
	address-bind install	Enables the address binding.
Configuring the IPv6 Address Binding Mode	⚠ (Optional) It is used to configure the IPv6 address binding mode.	
	address-bind ipv6-mode	Configures the IPv6 address binding mode.
Configuring the Exclude Port	⚠ (Optional) It is used to configure the exclude port.	
	address-bind uplink	Configures the exclude port.

1.4.1 Configuring Global IP-MAC Binding

Configuration Effect

- Configure a global IPv4-MAC binding.
- Enable the address binding function to control forwarding of the IPv4 or IPv6 packets.

Notes

- If you run the **address-bind install** command without IP-MAC binding configured, IP-MAC binding does not take effect and all packets are allowed to pass through.

Configuration Steps

↘ Configuring Global IP-MAC Binding

- (Mandatory) Perform this configuration in global configuration mode.

↘ Enabling the Address Binding Function

- (Mandatory) Perform this configuration in global configuration mode.

Verification

Run the **show running-config** or **show address-bind** command to check whether the configuration takes effect.

Related Commands

Configuring Global IP-MAC Binding

Command	**address-bind** { *ipv4-address* | *ipv6-address* } *mac-address*
Parameter Description	*ipv4-address*: indicates the bound IPv4 address. *ipv6-address*: indicates the bound IPv6 address. *mac-address*: indicates the bound MAC address.
Command Mode	Global configuration mode
Configuration Usage	Run this command to configure the binding relationship between an IPv4/IPv6 address and a MAC address. This command is not supported on ACs.

Enabling the Address Binding Function

Command	**address-bind install**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	Run this command to enable the global IP-MAC binding function. This function is used to control forwarding of IPv4 or IPv6 packets. This command is not supported on ACs.

Configuration Example

Configuring Global IP-MAC Binding and Enabling Address Binding

Configuration Steps	● Configure a global IPv4-MAC binding. ● Enable the address binding function.
	Hostname# configure terminal Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001 Hostname(config)# address-bind install
Verification	Display the global IP-MAC binding on the device.
	Hostname#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr ---------- ---------- 192.168.5.1 00d0.f800.0001

1.4.2 Configuring the IPv6 Address Binding Mode

Configuration Effect

- Change the IPv6 address binding mode so as to change the forwarding rules for IPv6 packets.

Configuration Steps

↘ Configuring the IPv6 Address Binding Mode

- (Optional) Perform this configuration when you want to change the forwarding rules for IPv6 packets.

Verification

- Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ Configuring the IPv6 Address Binding Mode

Command	**address-bind ipv6-mode** { **compatible** | **loose** | **strict** }
Parameter Description	**compatible**: indicates the compatible mode. **loose**: indicates the loose mode. **strict**: indicates the strict mode.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

↘ Configuring the IPv6 Address Binding Mode

Configuration Steps	• Configure a global IP-MAC binding. • Enable the address binding function. • Set the IPv6 address binding mode to Compatible.
	Hostname# configure terminal Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001 Hostname(config)# address-bind install Hostname(config)# address-bind ipv6-mode compatible
Verification	Run the **show running-config** command to display the configuration on the device.

1.4.3 Configuring the Exclude Port

Configuration Effect

- The address binding function is disabled on the exclude port, and all IP packets can be forwarded.

Notes

- The configuration can be performed only on a switching port or an L2 aggregate port.

Configuration Steps

Configuring the Exclude Port

- (Optional) Perform this configuration in global configuration mode when you want to disable the address binding function on a specified port.

Verification

Run the **show running-config** or **show address-bind uplink** command to check whether the configuration takes effect.

Related Commands

Configuring the Exclude Port

Command	**address-bind uplink** *interface-id*
Parameter Description	*interface-id*: indicates the ID of a switching port or an L2 aggregate port.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Configuring the Exclude Port

Configuration Steps	• Create a global IPv4-MAC binding. • Enable the address binding function. • Configure an exclude port.
	Hostname# configure terminal Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001 Hostname(config)# address-bind install Hostname(config)# address-bind uplink gigabitethernet 0/1
Verification	Display the global IP-MAC binding on the device.
	Hostname#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr --- --- 192.168.5.1 00d0.f800.0001 Hostname#show address-bind uplink Port State --- --- Gi0/1 Enabled Default Disabled

1.5 Monitoring

Displaying

Description	Command
Displays the IP-MAC binding on the device.	**show address-bind**
Displays the exclude port.	**show address-bind uplink**

1 Configuring IP Source Guard

1.1 Overview

The IP source guard function realizes hardware-based IP packet filtering to ensure that only the users having their information in the binding database can access networks normally, preventing users from forging IP packets.

1.2 Applications

Application	Description
Guarding Against IP/MAC Spoofing Attack	In network environments, users set illegal IP addresses and malicious users launch attacks through forging IP packets.

1.2.1 Guarding Against IP/MAC Spoofing Attack

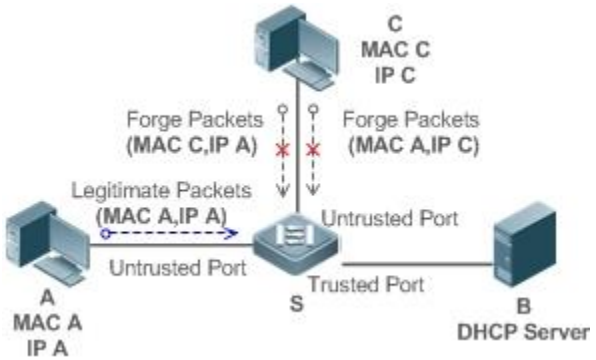
Scenario

Check the IP packets from DHCP untrusted ports. Forged IP packets will be filtered out based on the IP or IP-MAC field.

For example, in the following figure, the IP packets sent by DHCP clients are checked.

- The Source IP Address fields of IP packets should match DHCP-assigned IP addresses.
- The Source MAC Address fields of layer-2 packets should match the MAC addresses in DHCP request packets from clients.

Figure 1-1



Remarks:	S is a network access server (NAS). A and C are user PCs. B is a DHCP server within the control area.

Deployment

- Enable DHCP snooping on S to realize DHCP monitoring.
- Set all downlink ports on S as DHCP untrusted ports.
- Enable IP source guard on S to realize IP packet filtering.
- Enable IP–MAC match mode for IP source guard on S, filtering IP packets based on IP and MAC addresses.

1.3 Features

Basic Concepts

Source IP Address

Indicate the source IP address field of an IP packet.

Source MAC Address

Indicate the source MAC address field of an IP packet.

IP-based Filtering

Indicate a policy of IP packet filtering, where only the source IP addresses of all IP packets (except DHCP packets) passing through a port are checked. It is the default filtering policy of IP source guard.

IP-MAC based Filtering

A policy of IP packet filtering, where both the source IP addresses and source MAC addresses of all IP packets are checked, and only those user packets with these IP addresses and MAC addresses existing in the binding database are permitted.

Address Binding Database

As the basis of security control of the IP source guard function, the data in the address binding database comes from two ways: the DHCP snooping binding database and static configuration. When IP source guard is enabled, the data of the DHCP snooping binding database is synchronized to the address binding database of IP source guard, so that IP packets can be filtered strictly through IP source guard on a device with DHCP snooping enabled.

Excluded VLAN

By default, when IP source guard is enabled on a port, it is effective to all the VLANs under the port. Users may specify excluded VLANs, within which IP packets are not checked and filtered, which means that such IP packets are not controlled by IP source guard. At most 32 excluded VLANs can be specified for a port.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter the IP packets passing through ports by IP-based or IP-MAC based filtering.

1.3.1 Checking Source Address Fields of Packets

Filter the IP packets passing through ports based on source IP addresses or on both source IP addresses and source MAC addresses to prevent malicious attack by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to release such packets.

Working Principle

When IP source guard is enabled, the source addresses of packets passing through a port will be checked. The port can be a wired switching port, a layer-2 aggregate port (AP), or a layer-2 encapsulation sub-interface, or a WLAN interface. Such packets will pass the port only when the source address fields of the packets match the set of the address binding records generated by DHCP snooping, or the static configuration set by the administrator. There are two matching modes as below.

IP-based Filtering

Packets are allowed to pass a port only if the source IP address fields of them belong to the address binding database.

IP-MAC Based Filtering

Packets are allowed to pass a port only when both the layer-2 source MAC addresses and layer-3 source IP addresses of them match an entry in the address binding database.

Specifying Excluded VLAN

Packets within such a VLAN are allowed to pass a port without check or filtering.

Related Configuration

Enabling IP Source Guard on a Port

By default, the IP source guard is disabled on ports.

It can be enabled using the **ip verify source exclude-vlan** command.

Usually IP source guard needs to work with DHCP snooping. Therefore, DHCP snooping should also be enabled. DHCP snooping can be enabled at any time on Ruijie devices, either before or after IP source guard is enabled.

Configuring a Static Binding

By default, legal users passing IP source guard check are all from the binding database of DHCP snooping.

Bound users can be added using the **ip source binding** command.

Specifying an Excluded VLAN

By default, IP source guard is effective to all the VLANs under a port.

Excluded VLANs may be specified which are exempted from IP source guard using the **ip verify source** command.

Excluded VLANs can be specified only after IP source guard is enabled on a port. Specified excluded VLANs will be deleted automatically when IP source guard is disabled on a port.

The above-mentioned port can be a wired switching port, a layer-2 AP port or a layer-2 encapsulation sub-interface, or a WLAN interface.

1.4 Configuration

Configuration	Description and Command	
Configuring IP Source Guard	(Mandatory) It is used to enable IP source guard.	
	ip verify source	Enables IP source guard on a port.
	ip source binding	Configures a static binding.
	Ip verify source exclude-vlan	Specifies an excluded VLAN for IP source guard.

1.4.1 Configuring IP Source Guard

Configuration Effect

- Check the source IP addresses of input IP packets.

Notes

- When IP source guard is enabled, IP packets forwarding may be affected. In general case, IP source guard is enabled together with DHCP snooping.
- IP source guard cannot be configured on the trusted ports controlled by DHCP snooping.
- IP source guard cannot be configured on the global IP+MAC exclusive ports.
- IP source guard can be configured and enabled only on wired switch ports, Layer-2 AP ports, Layer-2 encapsulation sub-ports and WLAN. In a wired access scenario, it is supposed to be configured in the interface configuration mode. In a wireless access scenario, it is supposed to be configured in the WLAN security configuration mode.

Configuration Steps

- Enable DHCP snooping.
- Enable IP source guard.

Verification

Use the monitoring commands to display the address binding database of IP source guard.

Related Commands

Enabling IP Source Guard on a Port

Command	**ip verify source** [**port-security**]
Parameter	**port-security**: indicates IP-MAC based filtering.

Description	
Command	Interface configuration mode or WLAN security configuration mode
Usage Guide	Detection of users based on IP address or both IP and MAC addresses can be realized by enabling IP source guard for a port.

Configuring a Static Binding

Command	**ip source binding** *mac-address* **vlan** *vlan-id* **[***ip-address* **{ interface** *interface-type interface-number* **| wlan** *wlan-id* **| ip-mac | ip-only }**
Parameter Description	**mac-address:** indicates the MAC address of a static binding entry. **vlan-id:** indicates the VLAN ID of a static binding entry. It indicates the outer VLAN ID of a QINQ-termination user. **ip-address:** indicates the IP address of a static binding entry. *interface-type interface-number***:** indicates the port ID (PID) of a static binding entry. **wlan-id:** indicates the WLAN ID of a static binding entry. **ip-mac:** indicates the IP-MAC based mode. **ip-only:** indicates the IP-based mode.
Configuration Mode	Global configuration mode
Usage Guide	Through this command, legitimate users can pass IP source guard detection instead of being controlled by DHCP.

Specifying an Exception VLAN for IP Source Guard

Command	**ip verify source exclude-vlan** *vlan-id*
Parameter Description	**vlan-id:** indicates the VLAN ID exempted from IP source guard on a port.
Command	Interface configuration mode/WLAN security configuration mode
Usage Guide	By using this command, the specified VLANs under a port where IP source guard function is enabled can be exempted from check and filtering.

Configuration Example

Enabling IP Source Guard on Port 1

Configuration Steps	● Enable DHCP snooping. ● Enable IP source guard.
	Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip verify source Hostname(config-if-GigabitEthernet 0/1)# end Hostname(config)# wlansec 1 Hostname(config-wlansec)# ip verify source port-security Hostname(config-wlansec)# end
Verification	Displays the address filtering table of IP source guard.

Configuration Steps	● Enable DHCP snooping. ● Enable IP source guard.
	Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip verify source Hostname(config-if-GigabitEthernet 0/1)# end Hostname(config)# wlansec 1 Hostname(config-wlansec)# ip verify source port-security Hostname(config-wlansec)# end
Verification	Displays the address filtering table of IP source guard.
	Hostname# show ip verify source

Configuring a Static Binding

Configuration Steps	● Enable DHCP snooping. ● Enable IP source guard. ● Configure a static binding.
	Hostname# configure terminal Hostname(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3 Hostname(config)# end
Verification	Displays the address filtering table of IP source guard.
	Hostname# show ip verify source NO. INTERFACE FilterType FilterStatus IPADDRESS MACADDRESS VLAN TYPE ----- ---------- ---------- ---------- --------------- --------------- ---- ---------- 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 Static 2 GigabitEthernet 0/1 IP-ONLY Active Deny-All 3 WLAN 1 IP-MAC Active Deny-All

Configuring a Static Binding of a QINQ-Termination Product

Configuration Steps	● Enable DHCP snooping. ● Enable IP source guard. ● Configure a static binding.

	Hostname# configure terminal Hostname(config)# ip source binding 00d0.f801.0101 vlan 1 inner-vlan 10 192.168.4.243 interface GigabitEthernet 0/3 Hostname(config)# end
Verification	Displays the address filtering table of IP source guard.
	Hostname# show ip verify source NO. INTERFACE FILTERTYPE FILTERSTATUS IPADDRESS MACADDRESS VLAN INNER-VLAN TYPE ----- ---------- ---------- ---------- ---------- ---------- -------- -------- ---------- 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 10 Static

↘ Specifying an Excluded VLAN

Configuration Steps	● Enable DHCP snooping. ● Enable IP source guard.
	Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip verify source Hostname(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 Hostname(config-if)# end Hostname(config)# wlansec 1 Hostname(config-wlansec)# ip verify source Hostname(config-wlansec)# ip verify source exclude-vlan 1 Hostname(config-wlansec)# end
Verification	Display the configuration of excluded VLANs specified on a port.
	Hostname# show run

Common Errors

- Enable IP source guard on a trusted port under DHCP snooping.
- Specify an excluded VLAN before IP source guard is enabled.

1.5 Monitoring

Displaying

Description	Command

Displays the address filtering table of IP source guard.	**show ip verify source** [**interface** *interface-type interface-number* | **wlan** *wlan-id*]
Displays the address binding database of IP source guard.	**show ip source binding**

1 Configuring CPP

1.1 Overview

Malicious attacks are often found in network environment. Network devices are occupied with counterfeited management and protocol packets and have no time to process real management and protocol packets. In this way, the attacks bring destructive impacts on device security and network stability. The CPU Protect Policy (CPP) function protects CPU resources and important packets by means of packet identification and rate limiting.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Rate Limiting	Limits the rate of specified packets.

1.2.1 Rate Limiting

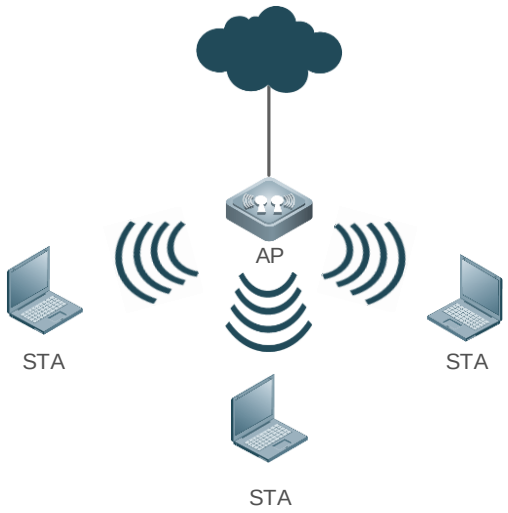
Scenario

The device is designed with the functions of packet identification and rate limiting, thus protecting the processors.

Figure 1-1 shows the networking topology of the CPP.

1. Multiple STAs access the AP.
2. Specified packet attacks (see Configuration for details) may occur on STAs in a network. The device must be able to protect their CPU.

Figure 1-1 Networking Topology

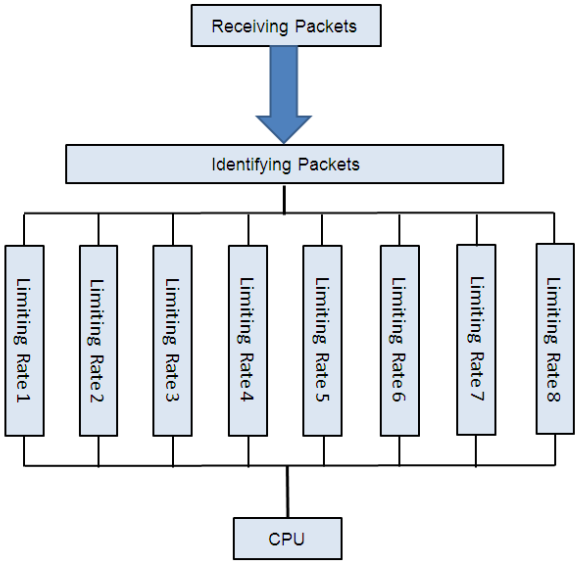


Deployment

Apply the CPP function on the AP to limit the rate of specified packets.

1.3 Features

Figure 1-2 Working Principle



Basic Concepts

↘ Identifying Packets

All packets that are sent to the AP for protocol processing must be classified (e.g., into ARP, BPDU and d1x) through packet identification (for the data classification of different products, see Configuration).

↘ Limiting Rate

An administrator can configure the rate limit for packets of each type, thus effectively dampening high-rate attack packets on the network.

Overview

Feature	Description
Identifying Packets	All packets that are sent to CPU are classified through packet identification.
Limiting Rate	High-rate attack packets are dampened by rate limiting.

1.3.1 Identifying Packets

All packets that are sent to CPU are classified through packet identification.

Working Principle

↘ Identifying Packets

CPP classifies packets and automatically applies the packet identification function by default.

1.3.2 Limiting Rate

An administrator can configure the rate limit for packets of each type, thus effectively dampening high-rate attack packets on the network.

Working Principle

↘ Limiting Rate

Packets that have been identified and classified are rate-limited, and packets that exceed the rate limit are discarded.

1.4 Configuration

Configuration	Description and Command	
Configuring the Rate Limit for Specified Packets	⚠ (Optional) It is used to set the rate limit for specified packets.	
	cpu-protect type	Sets the rate limit for specified packets

1.4.1 Configuring the Rate Limit for Specified Packets

Configuration Effect

- Configure the rate limit for various types of packets.

Notes

N/A

Configuration Steps

Configuring the Rate limit for Specified Packets

- Optional.
- Enable the CPP function on all APs unless otherwise specified.
- You can adjust the default rate limit for packets of each type as required.

Command	**cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** | **dhcp-realy-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **vrrp** } **pps** *value*
Parameter Description	**arp**: specifies the ARP packet. **bpdu**: specifies the IEEE BPDU packet. **capwap-disc**: specifies the CAPWAP DISCOVER packet. **d1x**: specifies the 802.1x EAPOL packet. **dhcp-option82**: specifies the DHCP OPTION82 packet. **dhcp-relay-client**: specifies the DHCP RELAY CLIENT packet. **dhcp-relay-server**: specifies the DHCP RELAY SERVER packet. **dhcps**: specifies the DHCP SNOOPING packet. **igmp**: specifies the IGMP packet. **ipmc**: specifies the IPv4 multicast packet. **ipv6-nans**: specifies the IPv6 neighbor discovery packet. **isis**: specifies the ISIS packet. **lldp**: specifies the LLDP packet. **ospf**: specifies the OSPF packet. **ospfv3**: specifies the OSPF version3 packet. **pppoe**: specifies the PPPOE packet. **pim**: specifies the PIM packet. **rip**: specifies the IPv4 RIP packet. **ripng**: specifies the IPv6 RIP packet. **vrrp**: specifies the VRRP packet. **pps** *value*: specifies the upper limit of packets per second, ranging from 0 to 148,810pps.
Defaults	The default values is 128.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show cpu-protect summary** command to display the configuration.

Configuration Example

N/A

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays the rate limit for packets of various types.	**show cpu-protect summary**
Displays statistics about specified packets.	**show cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** |**dhcp-realy-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **vrrp** }

1 Configuring NFPP

1.1 Overview

The Network Foundation Protection Policy (NFPP) provides guard for devices.

Some malicious attacks are always found in the network environment. These attacks bring heavy burdens to devices, resulting in high CPU usage and abnormal running on devices. These attacks are as follows:

Denial of service (DoS) attacks may greatly consume the memory, entries, or other resources of a device to cause system service unavailable.

Massive packet traffic is directed to the CPU, occupying the entire bandwidth of packets sent to the CPU. In this case, normal protocol traffic and management traffic cannot be processed by the CPU, causing protocol flapping or management failure. The forwarding on the data plane will also be affected and the entire network will become abnormal.

A great number of packets directed to the CPU consume massive CPU resources, making the CPU highly loaded and thereby causing device management failure or causing abnormal running.

NFPP can effectively protect the system from these attacks. Under attacks, NFPP protects proper running of various system services and keeps a low CPU load, thereby ensuring stable running of the entire network.

1.2 Applications

Application	Description
Attack Detection and Rate Limiting	Due to various malicious attacks such as ARP attacks and IP scanning attacks in the network, the CPU cannot process normal protocol and management traffic, causing protocol flapping or management failure. The NFPP attack detection and rate limiting function is used to limit the rate of attack traffic or isolate attack traffic so that the network can be recovered.
Centralized Rate Limiting and Distribution	Since normal service traffic is too large, you need to classify and prioritize the traffic. When a large number of packets are directed to the CPU, the CPU will be highly loaded, thereby causing device management or device running failure. The centralized rate limiting and distribution function is used to increase the priority of such traffic so that devices can run stably.

1.2.1 Attack Detection and Rate Limiting

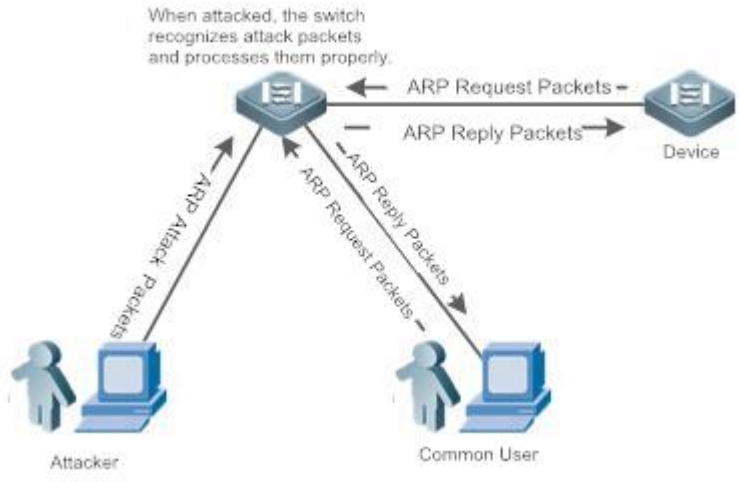
Scenario

NFPP supports attack detection and rate limiting for various types of packets, including Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Dynamic Host Configuration Protocol (DHCP) packets. It also allows users to define packet matching characteristics and corresponding attack detection and

rate limiting policies. The attack detection and rate limiting function takes effect based on each type of packets. This section uses ARP packets as an example to describe the scenario.

If an attacker sends ARP attack packets while the CPU capability is insufficient, a large number of CPU resources will be consumed for processing these ARP packets. If the attacker's ARP packet rate exceeds the maximum ARP bandwidth specified in the CPU Protect Policy (CPP) of the device, packet loss occurs among normal ARP packets. As shown in Figure 1-1, common users will fail to access the network, and the device will fail to send ARP responses to other devices.

Figure 1-1



Deployment

- By default, the ARP attack detection and rate limiting function is enabled, with corresponding policies configured. If an attacker's ARP packet rate exceeds the rate limit, the packets will be discarded. If the packet rate exceeds the attack threshold, a monitored host will be generated and prompt information will be output.
- If an attacker's ARP packet rate exceeds the rate limit defined in the CPP and affects normal ARP responses, you can enable attack isolation to discard ARP attack packets based on an ACL and recover the network.

For description of CPP configurations, refer to the "CPP" section.

To maximize the use of NFPP guard functions, modify the rate limits for various services in the CPP based on the application environment or use the configurations recommended by the system. You can run the **show cpu-protect summary** command to display the configurations.

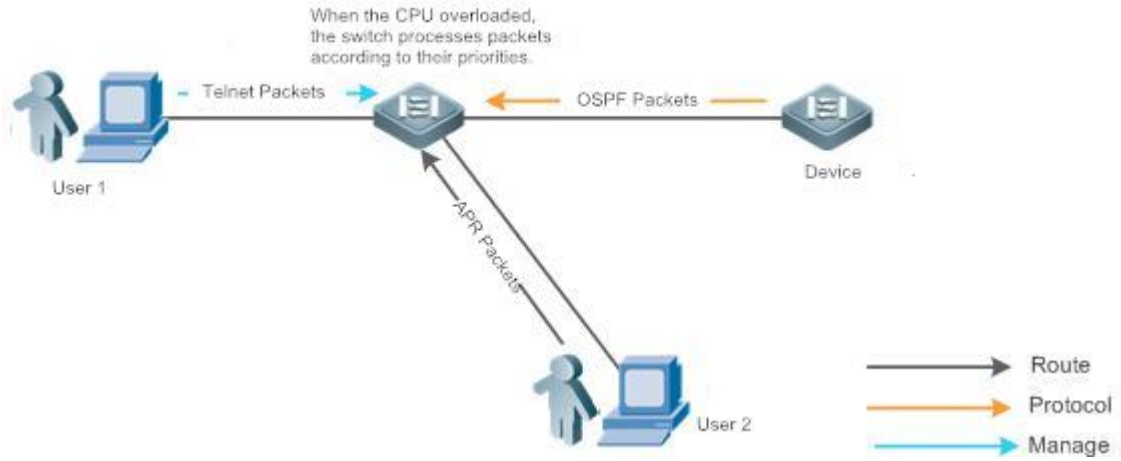
1.2.2 Centralized Rate Limiting and Distribution

Scenario

A device classifies services defined in the CPP into three types: Manage, Route, and Protocol. Each type of services has an independent bandwidth. Different types of services cannot share their bandwidths. Traffic exceeding the bandwidth threshold is discarded. By such service classification, service packets of a certain type can be processed first.

The device receives a large number of Telnet packets, OSPF packets, and ARP packets, causing CPU overload. In this case, the CPU cannot process all packets, and a large number of packets are backlogged in the queue, causing various problems such as occasional Telnet disconnection, OSPF protocol flapping, and ARP access failure to hosts.

Figure 1-2



Deployment

- By default, CPU centralized protection is enabled to assign an independent bandwidth and bandwidth ratio to each type of services. At the time, the CPU first processes Telnet packets to ensure uninterrupted connection of the Telnet service, and then processes OSPF packets to maintain OSPF protocol stability, and finally processes ARP packets.
- If the preceding problems occur in default configurations, you can accordingly adjust the bandwidth and bandwidth ratio for various types of services.

1.3 Features

Basic Concepts

↘ ARP Guard

In local area networks (LANs), IP addresses are converted to MAC addresses through ARP, which is significant for safeguarding network security. A large number of illegal ARP packets are sent to the gateway through the network, causing failure of the gateway to provide services for normal hosts. Such packets are called ARP-based DoS attacks. To prevent such attacks, limit the rate of ARP packets and detect and isolate the attack source.

↘ IP Anti-scanning

Many hacker attacks and network virus intrusions start from scanning active hosts in the network. Therefore, many scanning packets rapidly occupy the network bandwidth, causing network communication failure.

To solve this problem, Layer-3 devices provide IP guard to prevent scanning by hackers and Blaster Worm viruses and reduce the CPU load. Currently, there are mainly two types of IP attacks:

- Scanning destination IP address changes: As the greatest threat to the network, this type of attacks not only consumes network bandwidth and increases device load but also is a prelude of most hacker attacks.
- Sending IP packets to non-existing destination IP addresses at high rates: This type of attacks is mainly designed for consuming the CPU load. For a Layer-3 device, if the destination IP address exists, packets are directly forwarded by the switching chip without occupying CPU resources. If the destination IP address does not exist, IP packets are sent to the CPU, which then sends ARP requests to query the MAC address corresponding to the destination IP address. If too many packets are sent to the CPU, CPU resources will be consumed. This type of attacks is less destructive than the former ones.

To prevent the latter type of attacks, limit the rate of IP packets and detect and isolate the attack source.

↘ ICMP Guard

ICMP is a common approach for diagnosing network failures. After receiving an ICMP echo request from a host, the device returns an ICMP echo reply. The preceding process requires the CPU to process the packets, thereby definitely consuming part of CPU resources. If an attacker sends a large number of ICMP echo requests to the destination device, massive CPU resources will be consumed on the device, and the device may even fail to work properly. This type of attacks is called ICMP flood. To prevent this type of attacks, limit the rate of ICMP packets and detect and isolate the attack source.

↘ DHCP Guard

DHCP is widely used in LANs to dynamically assign IP addresses. It is significant for network security. Currently, the most common DHCP attacks, also called DHCP exhaustion attacks, use faked MAC addresses to broadcast DHCP requests. Various attack tools on the live network can easily complete this type of attacks. A network attacker can send sufficient DHCP requests to use up the address space provided by the DHCP server within a period. In this case, authorized hosts will fail to request DHCP IP addresses and thereby fail to access the network. To prevent this type of attacks, limit the rate of DHCP packets and detect and isolate the attack source.

↘ DHCPv6 Guard

DHCP version 6 (DHCPv6) is widely used in LANs to dynamically assign IPv6 addresses. Both DHCP version 4 (DHCPv4) and DHCPv6 have security problems. Attacks to DHCPv4 also apply to DHCPv6. A network attacker can send a large number of DHCPv6 requests to use up the address space provided by the DHCPv6 server within a period. In this case, authorized hosts will fail to request IPv6 addresses and therefore fail to access the network. To prevent this type of attacks, limit the rate of DHCPv6 packets and detect and isolate the attack source.

↘ ND Guard

Neighbor Discovery (ND) is mainly used in IPv6 networks to perform address resolution, router discovery, prefix discovery, and redirection. ND uses five types of packets: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect. These packets are called ND packets.

ND snooping monitors ND packets in the network to filter unauthorized ND packets. It also monitors IPv6 hosts in the network and binds the monitored IPv6 hosts to ports to prevent IPv6 address stealing. ND snooping requires ND packets to be sent to the CPU. If ND packets are sent at a very high rate, the CPU will be attacked. Therefore, ND guard must be provided to limit the rate of ND packets.

Overview

Feature	Description
Host-based Rate Limiting and Attack Identification	Limit the rate according to the host-based rate limit and identify host attacks in the network.
Port-based Rate Limiting and Attack Identification	Limit the rate according to the port-based rate limit and identify port attacks.
Configuring the Monitoring Period	Monitor host attackers in a specified period.
Configuring the Isolation Period	Isolate host attackers or port attackers in a specified period.
Configuring Trusted Hosts	Trust a host by not monitoring it.
Configuring Centralized Rate Limiting and Distributio	Classifies messages and differentiates processing priorities.

1.3.1 Host-based Rate Limiting and Attack Identification

Limit the rate of attack packets of hosts and identify the attacks.

Identify ARP scanning.

Identify IP scanning.

Working Principle

Hosts can be identified in two ways: based on the source IP address, VLAN ID, and port and based on the link-layer source MAC address, VLAN ID, and port. Each host has a rate limit and an attack threshold (also called alarm threshold). The rate limit must be lower than the attack threshold. If the attack packet rate exceeds the rate limit of a host, the host discards the packets beyond the rate limit. If the attack packet rate exceeds the attack threshold of a host, the host identifies host attacks, records them in logs, and sends Trap packets.

ARP scanning attacks may have occurred if ARP packets beyond the scanning threshold received in the configured period meet either of the following conditions:

- The link-layer source MAC address is fixed but the source IP address changes.
- The link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes.

Among IP packets beyond the scanning threshold received in the configured period, if the source IP address remains the same while the destination IP address continuously changes, IP scanning attack may have occurred.

When NFPP detects a specific type of attack packets under a service, it sends an alarm to the administrator. If the attack traffic persists, NFPP will not resend the alarm within 60 seconds after generating an alarm.

To prevent CPU resource consumption caused by frequent log printing, NFPP writes attack detection logs to the buffer, obtains them from the buffer at a specified rate, and prints them. NFPP does not limit the rate of Trap packets.

At present, only ARP guard and IP anti-scanning support anti-scanning.

1.3.2 Port-based Rate Limiting and Attack Identification

Limit the rate of port-based attack packets and identify the attacks.

Working Principle

Each port has a rate limit and an attack threshold. The rate limit must be lower than the attack threshold. If the packet rate exceeds the rate limit on a port, the port discards the packets. If the packet rate exceeds the attack threshold on a port, the port records the attacks in logs and sends Trap packets.

1.3.3 Configuring the Monitoring Period

Configures the monitoring period for an attacker.

Working Principle

Monitored hosts provide information about attackers in the current system. If the isolation period is 0 (that is, no isolation), the guard module automatically performs software monitoring on attackers in the configured monitoring period. Within the monitoring period, you can view the entries of a monitored host. If attacks are received from this host before aging of the monitoring period, refresh the monitoring period of the host; otherwise, when the monitoring period is aged to 0, the entries of the monitored host will be deleted. When the isolation time is configured to a non-0 value, the guard module automatically isolates the host monitored by the software.

1.3.4 Configuring the Isolation Period

Configure the isolation period for an attacker.

Working Principle

Isolation is performed by the guard policy after attacks are detected. Isolation is implemented using the filtering function of a software ACL to ensure that these attacks are not sent to the CPU, thereby ensuring proper running of the device.

The isolation function supports host-based and port-based isolation. When an attacker is isolated, a policy will be configured into an ACL. When the ACL resources are exhausted and isolation fails, logs will be printed to remind the administrator.

1.3.5 Configuring Trusted Hosts

Configure trusted hosts.

Working Principle

If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host will be allowed to send packets of specified types to the CPU.

1.3.6 Configuring Centralized Rate Limiting and Distributio

Set rate limits and percentages for three types of packets: Manage, Route, and Protocol.

Working Principle

Various services defined in the CPP are classified according to the principles of Manage, Route, and Protocol packets (as listed in the following table), each of which has a separate bandwidth. Different types of packets do not share bandwidth, and the flows exceeding the bandwidth threshold will be discarded. After classification, various service packets of a type are processed preferentially on the device.

NFPP allows an administrator to flexibly allocate the bandwidth of the three types of packets according to the actual network environment. This ensures the following two types of packets are preferentially processed: Protocol packets: Protocols can run properly. Manage packets: The administrator can implement normal management to guarantee normal operation of various important functions and improves the attack defense capability of the device.

After classification and rate limiting, all classified flows are grouped in one queue. When services of a type are processed inefficiently, packets corresponding to the service are stacked in the queue and may eventually exhaust the resources of the queue. NFPP allows an administrator to configure percentages of the three types of packets in a queue. When the queue length occupied by packets of a type exceeds the product of the total queue length and the percentage occupied by the packets of the type, the device discards the packets. This effectively solves the issue of queue resources occupied by packets of a type.

Packet Type	Service Type Defined in the CPU Protect Policy
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, gvrp, ripng, dvmrp, igmp, mpls, ospf, pim, pimv6, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c option82, tunnel-bpdu, and tunnel-gvrp
Route	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, and non-ip-packet-other
Manage	ip4-packet-local, ip6-packet-local, and arp

For more information about service types, see CPP configuration guide.

1.4 Configuration

Configuration	Description and Command	
Configuring ARP Guard	(Mandatory) It is used to configure the global ARP guard function.	
	arp-guard enable	Enables global attack detection.
	arp-guard monitor-period	Configures the monitoring period.
	arp-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	arp-guard rate-limit	Configures the global rate limit.
	arp-guard attack-threshold	Configures the global attack threshold.

Configuration	Description and Command	
	arp-guard scan-threshold	Configures the global host-based scanning threshold.
	⚠ (Optional) It is used to configure ARP isolation and ARP guard.	
	arp-guard isolate-period	Configures the global isolation period.
	arp-guard trusted-host	Configures trusted hosts.
	nfpp arp-guard enable	Enables attack detection for a port.
	nfpp arp-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp arp-guard scan-threshold	Configures the stage-by-stage scanning threshold for a port.
	nfpp arp-guard isolate-period	Configures the isolation period for a port.
Configuring IP Anti-scanning	⚠ (Mandatory) It is used to configure the global IP anti-scanning function.	
	ip-guard enable	Enables global attack detection.
	ip-guard monitor-period	Configures the monitoring period.
	ip-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	ip-guard rate-limit	Configures the global rate limit.
	ip-guard attack-threshold	Configures the global attack threshold.
	ip-guard scan-threshold	Configures the global host-based scanning threshold.
	⚠ (Optional) It is used to configure IP trusted hosts, IP isolation and port-based IP anti-scanning.	
	ip-guard isolate-period	Configures the global isolation period.
	ip-guard trusted-host	Configures trusted hosts.
	nfpp ip-guard enable	Enables attack detection for a port.
	nfpp ip-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp ip-guard scan-threshold	Configures the stage-by-stage scanning threshold for a port.
	nfpp ip-guard isolate-period	Configures the isolation period for a port.
Configuring ICMP Guard	⚠ (Mandatory) It is used to configure the global ICMP guard function.	
	icmp-guard enable	Enables global attack detection.
	icmp-guard monitor-period	Configures the monitoring period.
	icmp-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	icmp-guard rate-limit	Configures the global rate limit.
	icmp-guard attack-threshold	Configures the global attack threshold.

Configuration	Description and Command	
	(Optional) It is used to configure ICMP trusted hosts, ICMP isolation and port-based ICMP guard.	
	icmp-guard isolate-period	Configures the global isolation period.
	icmp-guard trusted-host	Configures trusted hosts.
	nfpp icmp-guard enable	Enables attack detection for a port.
	nfpp icmp-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp icmp-guard isolate-period	Configures the isolation period for a port.
Configuring DHCP Guard	(Mandatory) It is used to configure the global DHCP guard function.	
	dhcp-guard enable	Enables global attack detection.
	dhcp-guard monitor-period	Configures the monitoring period.
	dhcp-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	dhcp-guard rate-limit	Configures the global rate limit.
	dhcp-guard attack-threshold	Configures the global attack threshold.
	(Optional) It is used to configure DHCP isolation and port-based DHCP guard.	
	dhcp-guard isolate-period	Configures the global isolation period.
	dhcp-guard trusted-host	Configures trusted hosts.
	nfpp dhcp-guard enable	Enables attack detection for a port.
	nfpp dhcp-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp dhcp-guard isolate-period	Configures the isolation period for a port.
Configuring DHCPv6 Guard	(Mandatory) It is used to configure the global DHCPv6 guard function.	
	dhcpv6-guard enable	Enables global attack detection.
	dhcpv6-guard monitor-period	Configures the monitoring period.
	dhcpv6-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	dhcpv6-guard rate-limit	Configures the global rate limit.
	dhcpv6-guard attack-threshold	Configures the global attack threshold.
	(Optional) It is used to configure DHCPv6 isolation and DHCPv6 guard.	
	dhcpv6-guard isolate-period	Configures the global isolation period.
	dhcpv6-guard trusted-host	Configures trusted hosts.
	nfpp dhcpv6-guard enable	Enables attack detection for a port.
	nfpp dhcpv6-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp dhcpv6-guard isolate-period	Configures the isolation period for a port.

Configuration	Description and Command	
Configuring ND Guard	(Mandatory) It is used to configure the global ND guard function.	
	nd-guard enable	Enables global attack detection.
	nd-guard rate-limit	Configures the global rate limit.
	nd-guard attack-threshold	Configures the global attack threshold.
	(Optional) It is used to configure the port-based ND guard function.	
	nd-guard trusted-host	Configures trusted hosts.
	nfpp nd-guard enable	Enables attack detection for a port.
	nfpp nd-guard policy	Configures the rate limit and attack threshold for a port.
Configuring Centralized Rate Limiting and Distribution	(Mandatory) It is used to set the rate limits and bandwidth percentages of Manage, Route, and Protocol packets.	
	cpu-protect sub-interface pps	Configures the maximum bandwidth for packets of a type.
	cpu-protect sub-interface percent	Configures the maximum bandwidth percentage of a queue occupied by packets of a type.
Configuring NFPP Log Information	(Mandatory) It is used to set log information.	
	log-buffer entries	Configures the capacity of NFPP log buffer.
	log-buffer logs	Configures the rate when logs are obtained from the log buffer to generate system messages.
	(Optional) It is used to set logs to be recorded.	
	logging vlan	Configures the device to record logs of a specified VLAN.
	logging interface	Configures the device to record logs of a specified interface.

1.4.1 Configuring ARP Guard

Configuration Effect

- ARP attacks are identified based on hosts or ports. Host-based ARP attack identification supports two modes: identification based on the source IP address, VLAN ID, and port and identification based on the link-layer source MAC address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the ARP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ARP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

- ARP guard can also detect ARP scanning attacks. ARP scanning attacks indicate that the link-layer source MAC address is fixed but the source IP address changes, or that the link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes. Due to the possibility of misjudgment, hosts possibly performing ARP scanning are not isolated and are provided for the administrator's reference only.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.
- ARP guard prevents only ARP DoS attacks to the device, but not ARP spoofing or ARP attacks in the network.

Configuration Steps

↘ Enabling Attack Detection

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- If ARP guard is disabled, the system automatically clears monitored hosts, scanned hosts, and port isolation entries.

Command	**arp-guard enable**
Parameter Description	N/A
Defaults	ARP guard is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp arp-guard enable**
Parameter Description	N/A
Defaults	ARP guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ARP guard configured in interface configuration mode takes priority over that configured in global configuration mode.

↘ Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.

- Support the global configuration mode or interface configuration mode on the AP device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AP device.

Command	**arp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Configure the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AP device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete

monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.

- If the table of monitored hosts is full, the system prints the log "% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**arp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Attack Threshold

- Mandatory.
- To achieve the best ARP guard effect, you are advised to configure the host-based rate limit and alarm threshold based on the following rules: Source IP address-based rate limit < Source IP address-based alarm threshold < Source MAC address-based rate limit < Source MAC address-based alarm threshold.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over source IP address-based rate limiting while the latter takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **arp-guard rate-limit** {**per-src-ip** | **per-src-mac**} *pps* command to configure rate limits of hosts identified based on the source IP address, VLAN ID, and port and of hosts identified based on the link-layer source MAC address, VLAN ID, and port.
- In NFPP configuration mode: run the **arp-guard attack-threshold** {**per-src-ip** | **per-src-mac**} *pps* command to configure attack thresholds of hosts identified based on the source IP address, VLAN ID, and port and of hosts identified based on the link-layer source MAC address, VLAN ID, and port.
- In interface configuration mode: run the **nfpp arp-guard policy** {**per-src-ip | per-src-mac**} *rate-limit-pps attack-threshold-pps* command to configure rate limits and attack thresholds of hosts identified based on the source IP address, VLAN ID, and port and of hosts identified based on the link-layer source MAC address, VLAN ID, and port on an interface.

Command	**arp-guard rate-limit** { **per-src-ip**	**per-src-mac**	**per-port** } *pps*
Parameter Description	**per-src-ip:** Limits the rate for each source IP address. **per-src-mac:** Limits the rate of packets from each source MAC address.

	per-port: Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For AP devices, the default rate limit for packets based on source IP address/source MAC address is 30 pps, and the default rate limit for packets based on port is 240 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-src-mac:** Configures the attack threshold for each source MAC address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is packets per second (pps).
Defaults	For AP devices, the default rate limit for packets based on source IP address/source MAC address is 60 pps, and the default rate limit for packets based on port is 480 pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Command	**nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip:** Configures the rate limit and attack threshold for each source IP address. **per-src-mac:** Configures the rate limit and attack threshold for each source MAC address. **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Scanning Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- The ARP scanning table stores only the latest 256 records. When the ARP scanning table is full, the latest record will overwrite the earliest record.
- ARP scanning attack may have occurred if ARP packets received within 10 seconds meet either of the following conditions:
  - The link-layer source MAC address is fixed but the source IP address changes.
  - The link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes, and the change times exceed the scanning threshold.

Command	**arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	The default scanning threshold is 100 in the unit of 10 seconds.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	By default, no port-based ARP scanning threshold is configured and the global ARP scanning threshold is used.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For ARP guard, you can configure only a maximum of 500 IP addresses and MAC addresses not to be monitored.
- Support the global configuration mode on the AP device.
- If any entry matching a trusted host (the IP addresses and MAC addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.1 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.1 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 1.1.1.1 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.1 0000.0000.1111 is not found." to notify the administrator.

Command	**arp-guard trusted-host** *ip mac*
Parameter Description	*ip*: Indicates the IP address. *mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host

	to be trusted. This trusted host can send ARP packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends ARP attack packets to a device configured with ARP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on ARP Guard

Scenario	● ARP host attacks exist in the system, and some hosts fail to properly establish an ARP connection. ● ARP scanning exists in the system, causing a very high CPU usage. ● ARP packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Set the host-based attack threshold to 5 pps. ● Set the ARP scanning threshold to 10 pps. ● Set the isolation period to 180 pps. ● Configure trusted hosts.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#arp-guard rate-limit per-src-mac 5 Hostname (config-nfpp)#arp-guard attack-threshold per-src-mac 10 Hostname (config-nfpp)#arp-guard isolate-period 180 Hostname (config-nfpp)#arp-guard trusted-host 1.1.1.1 0000.0000.1111
Verification	● Run the **show nfpp arp-guard summary** command to display the configurations.
	Hostname# show nfpp arp-guard summary (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold Global Disable 180 4/5/100 8/10/200 15 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp arp-guard hosts** command to display monitored hosts.

	Hostname# show nfpp arp-guard hosts If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address MAC address remain-time(s) ---- --------- ---------- ---------- -------------- 1 Gi0/43 5.5.5.16 - 175 Total: 1 host
	● Run the **show nfpp arp-guard scan** command to display scanned hosts.
	Hostname# show nfpp arp-guard scan VLAN interface IP address MAC address timestamp ---- --------- ---------- ---------- --------- 1 Gi0/5 - 001a.a9c2.4609 2013-4-30 23:50:32 1 Gi0/5 192.168.206.2 001a.a9c2.4609 2013-4-30 23:50:33 1 Gi0/5 - 001a.a9c2.4609 2013-4-30 23:51:33 1 Gi0/5 192.168.206.2 001a.a9c2.4609 2013-4-30 23:51:34 Total: 4 record(s)
	● Run the **show nfpp arp-guard trusted-host** command to display trusted hosts.
	Hostname# show nfpp arp-guard trusted-host IP address mac ---------- ---- 1.1.1.1 0000.0000.1111 Total: 1 record(s)

1.4.2 Configuring IP Anti-scanning

Configuration Effect

- IP attacks are identified based on hosts or ports. In host-based IP attack identification, IP attacks are identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the IP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the IP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.
- IP guard can also detect IP scanning attacks. IP anti-scanning applies to IP packet attacks as follows: the destination IP address continuously changes but the source IP address remains the same, and the destination IP address is not the IP address of the local device.
- IP anti-scanning applies to IP packet attacks where the destination IP address is not the local IP address. The CPP limits the rate of IP packets where the destination IP address is the local IP address.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

↘ Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AP device.
- If IP anti-scanning is disabled, the system automatically clears monitored hosts.

Command	**ip-guard enable**
Parameter Description	N/A
Defaults	IP anti-scanning is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp ip-guard enable**
Parameter Description	N/A
Defaults	IP anti-scanning is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	IP anti-scanning configured in interface configuration mode takes priority over that configured in global configuration mode.

↘ Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.

Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AP device.

Command	**ip-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AP device.
- If the number of monitored hosts reaches 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**ip-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **ip-guard rate-limit** { **per-src-ip** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **ip-guard attack-threshold** { **per-src-ip** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp ip-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**ip-guard rate-limit** { **per-src-ip**	**per-port** } *pps*
Parameter Description	**per-src-ip:** Limits the rate for each source IP address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	**per-src-ip**: 20 pps. **per-port**: 1,000 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**ip-guard attack-threshold** { **per-src-ip**	**per-port** } *pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	**per-src-ip**: 20 pps. **per-port**: 1,500 pps.

Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Command	**nfpp ip-guard policy** { **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-port:** Configures the attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Scanning Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- IP scanning attack may have occurred if IP packets received within 10 seconds meet the following conditions:
  - The source IP address remains the same.
  - The destination IP address continuously changes and is not the local IP address, and the change times exceed the scanning threshold.

Command	**ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	The default scanning threshold is 100 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	By default, no port-based IP scanning threshold is configured and the global IP scanning threshold is used.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.

- For IP anti-scanning, you can configure a maximum of 500 IP addresses not to be monitored.
- Support the global configuration mode on the AP device.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.

Command	**ip-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send IP packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends IP attack packets to a device configured with IP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on IP Guard

Scenario	● IP host attacks exist in the system, and packets of some hosts cannot be properly routed and forwarded. ● IP scanning exists in the system, causing a very high CPU usage. ● Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuratio	● Configure the host-based attack threshold.

n Steps	● Configure the IP scanning threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#ip-guard rate-limit per-src-ip 20 Hostname (config-nfpp)#ip-guard attack-threshold per-src-ip 30 Hostname (config-nfpp)#ip-guard isolate-period 180 Hostname (config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255
Verification	● Run the **show nfpp ip-guard summary** command to display the configurations.
	Hostname# show nfpp ip-guard summary (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold Global Disable 180 20/-/100 30/-/200 100 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp ip-guard hosts** command to display monitored hosts.
	Hostname# show nfpp ip-guard hosts If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address Reason remain-time(s) ---- --------- ---------- ------ -------------- 1 Gi0/5 192.168.201.47 ATTACK 160 Total: 1 host
	● Run the **show nfpp ip-guard trusted-host** command to display trusted hosts.
	Hostname# show nfpp ip-guard trusted-host IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

1.4.3 Configuring ICMP Guard

Configuration Effect

- ICMP attacks are identified based on hosts or ports. In host-based attack identification, ICMP attacks are identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the ICMP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ICMP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

↘ Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AP device.
- If ICMP guard is disabled, the system automatically clears monitored hosts.

Command	**icmp-guard enable**
Parameter Description	N/A
Defaults	ICMP guard is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp icmp-guard enable**
Parameter Description	N/A
Defaults	ICMP guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ICMP guard configured in interface configuration mode takes priority over that in global configuration mode.

↘ Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AP device.

- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Command	**nfpp icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AP device.

Command	**icmp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs isolation against attackers monitored by software and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AP device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**icmp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ICMP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps* command to configure the global rate limit.

- In NFPP configuration mode: run the **icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp icmp-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Limits the rate for each source IP address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	**per-src-ip**: 200 pps; **per-port**: 400 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	**per-src-ip**: 200 pps; **per-port**: 400 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp icmp-guard policy** { **per-src-ip	per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip:** Configures the rate limit and attack threshold for each source IP address. **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For ICMP anti-scanning, you can configure a maximum of 500 IP addresses not to be monitored.
- Support the global configuration mode on the AP device.

- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.

Command	**icmp-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send ICMP packets to the CPU, without any rate limiting or alarm reporting. You can configure the mask so that no host in one network segment is monitored. You can configure a maximum of 500 trusted hosts.

Verification

When a network host sends ICMP attack packets to a device configured with ICMP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on ICMP Guard

Scenario	• ICMP host attacks exist in the system, and some hosts cannot successfully ping devices. • Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	• Configure the host-based attack threshold. • Set the isolation period to a non-zero value. • Configure trusted hosts.

	Hostname# configure terminal Hostname(config)# nfpp Hostname(config-nfpp)#icmp-guard rate-limit per-src-ip 20 Hostname(config-nfpp)#icmp-guard attack-threshold per-src-ip 30 Hostname(config-nfpp)#icmp-guard isolate-period 180 Hostname(config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255
Verification	● Run the **show nfpp icmp-guard summary** command to display the configurations.
	Hostname# show nfpp icmp-guard summary (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Global Disable 180 20/-/400 30/-/400 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp icmp-guard hosts** command to display monitored hosts.
	Hostname# show nfpp icmp-guard hosts If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address remain-time(s) ---- --------- ---------- ---------- 1 Gi0/5 192.168.201.47 160 Total: 1 host
	● Run the **show nfpp icmp-guard trusted-host** command to display trusted hosts.
	Hostname# show nfpp icmp-guard trusted-host IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

1.4.4 Configuring DHCP Guard

Configuration Effect

- DHCP attacks are identified based on hosts or ports. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the DHCP packet rate exceeds the rate limit, the

packets beyond the rate limit are discarded. If the DHCP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AP device.
- If DHCP guard is disabled, the system automatically clears monitored hosts.

Command	**dhcp-guard enable**
Parameter Description	N/A
Defaults	Attack detection is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp dhcp-guard enable**
Parameter Description	N/A
Defaults	DHCP guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	DHCP guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**dhcp-guard isolate-period** [*seconds* | **permanent**]

Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Command	**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AP device.

Command	**dhcp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs isolation against attackers monitored by software and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.

- Support the global configuration mode on the AP device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**dhcp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **dhcp-guard rate-limit** { **per-src-mac** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **dhcp-guard attack-threshold** { **per-src-mac** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.

- In interface configuration mode: run the **nfpp dhcp-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**dhcp-guard rate-limit** { **per-src-mac** | **per-port** } *pps*
Parameter Description	**per-src-mac:** Limits the rate for each source MAC address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AP devices, the default rate limit for packets based on source MAC address is 5 pps, and the default rate limit for packets based on port is 150 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**dhcp-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*
Parameter Description	**per-src-mac:** Configures the attack threshold for each source MAC address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AP devices, the default rate limit for packets based on source MAC address is 10 pps, and the default rate limit for packets based on port is 300 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp dhcp-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-mac:** Configures the rate limit and attack threshold for each source MAC address**.** **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For DHCP guard, you can configure a maximum of 500 MAC addresses not to be monitored.
- Support the global configuration mode on the AP device.
- If any entry matching a trusted host (MAC addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.

- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 0000.0000.1111 is not found." to notify the administrator.

Command	**dhcp-guard trusted-host** *mac*
Parameter Description	*mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send DHCP packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends DHCP attack packets to a device configured with DHCP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on DHCP Guard

Scenario	DHCP host attacks exist in the system, and some hosts fail to request IP addresses. DHCP packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	• Configure the host-based attack threshold. • Set the isolation period to a non-zero value. • Configure trusted hosts.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#dhcp-guard rate-limit per-src-mac 8

	Hostname (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16 Hostname (config-nfpp)#dhcp-guard isolate-period 180 Hostname (config-nfpp)#dhcp-guard trusted-host 0000.0000.1111
Verification	● Run the **show nfpp dhcp-guard summary** command to display the configurations.
	Hostname# show nfpp dhcp-guard summary (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Global Disable 180 -/8/150 -/16/300 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp dhcp-guard hosts** command to display monitored hosts.
	Hostname# show nfpp dhcp-guard hosts If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 001a.a9c2.4609 160 Total: 1 host
	● Run the **show nfpp dhcp-guard trusted-host** command to display trusted hosts.
	Hostname# show nfpp dhcp-guard trusted-host mac ---- 0000.0000.1111 Total: 1 record(s)

1.4.5 Configuring DHCPv6 Guard

Configuration Effect

- DHCPv6 attacks are identified based on hosts or ports. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the DHCPv6 packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCPv6 packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets.
- In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AP device.
- If DHCPv6 guard is disabled, the system automatically clears monitored hosts.

Command	**dhcpv6-guard enable**
Parameter Description	N/A
Defaults	Attack detection is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp dhcpv6-guard enable**
Parameter Description	N/A
Defaults	DHCPv6 guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	DHCPv6 guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.

Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Command	**nfpp dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AP device.

Command	**dhcpv6-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs isolation against attackers monitored by software and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AP device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete

monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.

- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**dhcpv6-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp dhcpv6-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**dhcpv6-guard rate-limit** { **per-src-mac**	**per-port** } *pps*
Parameter	**per-src-mac:** Limits the rate for each source MAC address.

Description	**per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AP devices, the default rate limit for packets based on source MAC address is 5 pps, and the default rate limit for packets based on port is 150 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*
Parameter Description	**per-src-mac:** Configures the attack threshold for each source MAC address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AP devices, the default rate limit for packets based on source MAC address is 10 pps, and the default rate limit for packets based on port is 300 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-mac:** Configures the rate limit and attack threshold for each source MAC address. **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For DHCPv6 guard, you can configure a maximum of 500 MAC addresses not to be monitored.
- Support the global configuration mode on the AP device.
- If any entry matching a trusted host (MAC addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 0000.0000.1111." to notify the administrator.

- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 0000.0000.1111 is not found." to notify the administrator.

Command	**dhcpv6-guard trusted-host** *mac*
Parameter Description	*mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send DCHPv6 packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends DHCPv6 attack packets to a device configured with DHCPv6 attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If an isolation entry needs to be created for the attacker, attacker isolation prompt information is displayed.

Configuration Example

↘ CPU Protection Based on DHCPv6 Guard

Scenario	DHCPv6 host attacks exist in the system, and DHCPv6 neighbor discovery fails on some hosts. DHCPv6 packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	• Configure the host-based attack threshold. • Set the isolation period to a non-zero value. • Configure trusted hosts.
	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8 Hostname (config-nfpp)#dhcpv6-guard attack-threshold per-src-mac 16 Hostname (config-nfpp)#dhcpv6-guard isolate-period 180 Hostname (config-nfpp)#dhcpv6-guard trusted-host 0000.0000.1111

Verification	● Run the **show nfpp dhcpv6-guard summary** command to display the configurations.
	Hostname# show nfpp dhcpv6-guard summary (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) Interface Status Isolate-period Rate-limit Attack-threshold Global Disable 180 -/8/150 -/16/300 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp dhcpv6-guard hosts** command to display monitored hosts.
	Hostname# show nfpp dhcpv6-guard hosts If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 001a.a9c2.4609 160 Total: 1 host
	● Run the **show nfpp dhcpv6-guard trusted-host** command to display trusted hosts.
	Hostname# show nfpp dhcpv6-guard trusted-host mac ---- 0000.0000.1111 Total: 1 record(s)

1.4.6 Configuring ND Guard

Configuration Effect

- AR ND guard classifies ND packets into three types based on their purposes: 1. NS and NA; 2. RS; 3. RA and Redirect. The first type of packets are used for address resolution. The second type of packets are used by hosts to discover the gateway. The third type of packets are related to routing: RAs are used to advertise the gateway and prefix while Redirect packets are used to advertise a better next hop.
- At present, only port-based ND packet attack identification is supported. You can configure the rate limits and alarm thresholds for these three types of packets. If the ND packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ND packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AP device.

Command	**nd-guard enable**
Parameter Description	N/A
Defaults	ND guard is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp nd-guard enable**
Parameter Description	N/A
Defaults	ND guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ND guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AP device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ND_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- In NFPP configuration mode: run the **nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.

- In interface configuration mode: run the **nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na:** Indicates NSs and NAs. **rs:** Indicates RSs. **ra-redirect:** Indicates RAs and Redirect packets. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AP devices, the default attack threshold for ns-na, rs, and ra-redirect packets is 15 pps.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na**: Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AP devices, the default attack threshold for ns-na, rs, and ra-redirect packets is 30 pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Command	**nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*
Parameter Description	**ns-na:** Indicates NSs and NAs. **rs**: Indicates RSs. **ra-redirect**: Indicates RAs and Redirect packets. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit. ND snooping classifies ports into two types: untrusted ports (connecting the host) and trusted ports (connecting to the gateway). As traffic on a trusted port is usually larger than that on an untrusted port, the rate limit for a trusted port is higher than that for an untrusted port. If ND snooping is enabled for a trusted port, ND snooping sets the rate limit to 800 pps and the attack threshold to 900 pps for the three types of packets on the port by advertising ND guard. ND guard treats the rate limit configured for ND snooping and that configured by the administrator in the same way. The value configured later overwrites the value configured earlier and is stored in the configuration file. The attack threshold configured for ND snooping is treated in a similar way.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For ND guard, you can configure a maximum of 500 MAC addresses not to be monitored.
- Support the global configuration mode on the AP device.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 0000.0000.1111 is not found." to notify the administrator.

Command	**nd-guard trusted-host** *mac*
Parameter Description	*mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send ND packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends ND attack packets to a device configured with ND attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold for a port, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

CPU Protection Based on ND Guard

Scenario	ND host attacks exist in the system, and neighbor discovery fails on some hosts. ND packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	• Configure the host-based attack threshold.

	Hostname# configure terminal Hostname(config)# nfpp Hostname (config-nfpp)# nd-guard rate-limit per-port ns-na 30 Hostname (config-nfpp)# nd-guard attack-threshold per-port ns-na 50 Hostname (config-nfpp)#nd-guard trusted-host 0000.0000.1111
Verification	● Run the **show nfpp nd-guard summary** command to display the configurations.
	Hostname# show nfpp nd-guard summary (Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.) Interface Status Rate-limit Attack-threshold Global Disable 30/15/15
	● Run the **show nfpp nd-guard trusted-host** command to display trusted hosts.
	Hostname# show nfpp nd-guard trusted-host mac ---- 0000.0000.1111 Total: 1 record(s)

1.4.7 Configuring Centralized Rate Limiting and Distribution

Configuration Effect

The centralized rate limiting and distribution technology solves the problem of preferential processing of Manage and Protocol packets when the network is busy.

Notes

The value range for the bandwidth percentage of a queue occupied by packets of a type must be less than or equal to 100% minus the difference between the sum of the bandwidth percentages of packets of the other two types.

Configuration Steps

↘ Configuring the Maximum Bandwidth for Packets of a Type

Mandatory. The default traffic bandwidth for Manage, Route, and Protocol packets are the same.

This function can be configured globally on an AP.

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **pps** *pps-vaule*
Parameter Description	**manage**: specifies Manage packets. **protocol**: specifies Protocol packets.

	route: specifies Route packets. *pps-value*: specifies the rate limit. The value range is 1–100000.
Defaults	The default value of an AP is **3000**.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Bandwidth Percentage of a Queue Occupied by Packets of a Type

Mandatory. By default, Manage, Route, and Protocol packets occupy 30%, 40%, and 25% bandwidths of a queue.

This function can be configured globally on an AP.

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **percent** *percent-vaule*
Parameter Description	**manage**: specifies Manage packets. **protocol**: specifies Protocol packets. **route**: specifies Route packets. *percent-value*: specifies the bandwidth percentage. The value range is 1–100.
Defaults	manage: 30% protocol: 25% route: 40%
Command Mode	Global configuration mode
Usage Guide	The value range for the bandwidth percentage of a queue occupied by packets of a type must be less than or equal to 100% minus the difference between the sum of the bandwidth percentages of packets of the other two types.

Verification

N/A

Configuration Example

Configuring Centralized Rate Limiting and Distribution to Classify Priorities of Packets Sent to the CPU

Scenario	● There are various packets with a high traffic volume on a network, and the packets fall into different centralized categories.
Configuration Steps	● Configure the maximum bandwidth for packets of a type. ● Configure the maximum bandwidth percentage of a queue occupied by packets of a type.
	Hostname# configure terminal Hostname(config)# cpu-protect sub-interface manage pps 5000 Hostname(config)# cpu-protect sub-interface manage percent 25
Verification	N/A

Common Errors

N/A

1.4.8 Configuring NFPP Log Information

Configuration Effect

NFPP obtains a log from the dedicated log buffer at a certain rate, generates a system message, and clears this log from the dedicated log buffer.

Notes

Logs are continuously printed in the log buffer, even if attacks have stopped.

Configuration Steps

↘ Configuring the Log Buffer Capacity

- Mandatory.
- If the log buffer is full, new logs are discarded and a corresponding prompt is displayed.
- If the log buffer overflows, subsequent logs are discarded and an entry with all attributes marked with a hyphen (-) is displayed in the log buffer. The administrator needs to increase the log buffer capacity or the system message generation rate.
- Support the global configuration mode on the AP device.

Command	**log-buffer entries** *number*
Parameter Description	*number*: Indicates the buffer size in unit of the number of logs, ranging from 0 to 1024.
Defaults	The default buffer size is 256.
Command Mode	NFPP configuration mode
Usage Guide	-

↘ Configuring the System Message Generation Rate

- Mandatory.
- The system message generation rate depends on two parameters: the time segment length and the number of system messages generated in the time segment.
- If both of the preceding two parameters are set to 0, system messages are immediately generated for logs but are not stored in the log buffer.
- Support the global configuration mode on the AP device.

Command	**log-buffer logs** *number_of_message* **interval** *length_in_seconds*
Parameter Description	*number_of_message*: Ranges from 0 to 1,024. The value 0 indicates that all logs are recorded in the log buffer and no system message is generated. *length_in_seconds*: Ranges from 0 to 86,400 (1 day). The value **0** indicates that logs are not recorded in the log buffer but system messages are instantly generated. This also applies to *number_of_message* and *length_in_seconds*. *number_of_message/length_in_second:* Indicates the system message generation rate.

Defaults	The default value of *number_of_message* is 1 and the default value of *length_in_seconds* is 30.
Command Mode	NFPP configuration mode
Usage Guide	

Enabling Log Filtering

- (Optional) Log filtering is disabled by default.
- Logs can be filtered based on a port or VLAN.
- If log filtering is enabled, logs not meeting the filtering rule are discarded.
- Support the global configuration mode on the AP device.

Command	**logging vlan** *vlan-range*
Parameter Description	*vlan-range*: Records logs in a specified VLAN range. The value format is "1-3,5 for example.
Defaults	All logs are recorded by default.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs in the specified VLAN range are recorded. Between port-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Command	**logging interface** *interface-id*
Parameter Description	*interface-id*: Records logs of a specified port.
Defaults	All logs are recorded by default.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs of the specified port are recorded. Between port-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Configuration Example

CPU Protection Based on ND Guard

Scenario	● If there are too many attackers, log printing will affect the usage of user interfaces and must be restricted.
Configuration Steps	● Configure the log buffer capacity. ● Configure the system message generation rate. ● Configure VLAN-based log filtering.
	Hostname# configure terminal Hostname(config)# nfpp

	Hostname (config-nfpp)#log-buffer entries 1024 Hostname (config-nfpp)#log-buffer logs 3 interval 5 Hostname (config-nfpp)#logging interface vlan 1
Verification	● Run the **show nfpp log summary** command to display the configurations.
	Hostname# show nfpp log summary Total log buffer size : 1024 Syslog rate : 3 entry per 5 seconds Logging: VLAN 1
	● Run the **show nfpp log buffer** command to display logs in the log buffer.
	Hostname# show nfpp log buffer Protocol VLAN Interface IP address MAC address Reason Timestamp -------- ---- --------- ---------- ---------- ------ --------- ARP 1 Gi0/5 192.168.206.2 001a.a9c2.4609 SCAN 2013-5-1 5:4:24

1.5 Monitoring

Clearing

Description	Command
Clears the ARP guard scanning table.	**clear nfpp arp-guard scan**
Clears monitored hosts in ARP guard.	**clear nfpp arp-guard hosts**
Clears monitored hosts in IP guard.	**clear nfpp ip-guard hosts**
Clears monitored hosts in IMCP guard.	**clear nfpp icmp-guard hosts**
Clears monitored hosts in DHCP guard.	**clear nfpp dhcp-guard hosts**
Clears monitored hosts in DHCPv6 guard.	**clear nfpp dhcpv6-guard hosts**
Clears logs.	**clear nfpp log**

Displaying

Description	Command
Displays configuration parameters of ARP guard.	**show nfpp arp-guard summary**

Description	Command
Displays monitored hosts of ARP guard.	**show nfpp arp-guard hosts**
Displays the ARP guard scanning table.	**show nfpp arp-guard scan**
Displays trusted hosts in ARP guard.	**show nfpp arp-guard trusted-host**
Displays configuration parameters of IP guard.	**show nfpp ip-guard summary**
Displays monitored hosts in IP guard.	**show nfpp ip-guard hosts**
Displays trusted hosts in IP guard.	**show nfpp ip-guard trusted-host**
Displays configuration parameters of ICMP guard.	**show nfpp icmp-guard summary**
Displays monitored hosts in ICMP guard.	**show nfpp icmp-guard hosts**
Displays trusted hosts in ARP guard.	**show nfpp icmp-guard trusted-host**
Displays configuration parameters of DHCP guard.	**show nfpp dhcp-guard summary**
Displays monitored hosts in DHCP guard.	**show nfpp dhcp-guard hosts**
Displays trusted hosts in DHCP guard.	**show nfpp dhcp-guard trusted-host**
Displays configuration parameters of DHCPv6 guard.	**show nfpp dhcpv6-guard summary**
Displays monitored hosts in DHCPv6 guard.	**show nfpp dhcpv6-guard hosts**
Displays trusted hosts in DHCPv6 guard.	**show nfpp dhcpv6-guard trusted-host**
Displays configuration parameters of ND guard.	**show nfpp nd-guard summary**
Displays trusted hosts in ND guard.	**show nfpp nd-guard trusted-host**
Displays NFPP logs.	**show nfpp log summary**
Displays the NFPP log buffer.	**show nfpp log buffer** [**statistics**]

1 Configuring Password Policies

1.1 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

1.2 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.

1.3 Configuration

Configuration	Description and Command	
Configuring Basic Function of 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.

1.3.1 Configuring Basic Function of Password Security Policy

Configuration Effect

- 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** *days*
Parameter Description	**life-cycle** *days*: Indicates the password life cycle in the unit of days. The value range is from 1 to 65535.
Command	Global configuration mode

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** *length*
Parameter Description	**min-size** *length*: Indicates the minimum length of passwords. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the minimum length of passwords. If the minimum length of passwords is not configured, users can input a password of any length.

Setting the No-Repeat Times of Latest Password Configuration

Command	**password policy no-repeat-times** *times*
Parameter Description	**no-repeat-times** *times*: Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, all old passwords used in the several times of latest password configuration will be recorded as the user's password history records. If the new password input by the user has been used previously, the system gives an error prompt and the password modification fails. You can configure the maximum number of password history records per user. When the number of password history records of a user is greater than the maximum number configured for the user, the new password history record will overwrite the user's oldest password history record.

Enabling the Strong Password Detection Function

Command	**password policy strong**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the strong password detection function is enabled, a prompt is displayed for the following types of passwords: 1. Passwords that are the same as corresponding accounts; 2. Simple passwords that contain characters or digits only.

Setting the Storage of Encrypted Passwords

Command	**service password-encryption**
Parameter	N/A

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	N/A
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: 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	● 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.
	Hostname# configure terminal Hostname(config)# password policy min-size 8 Hostname(config)# password policy life-cycle 90 Hostname(config)# service password-encryption Hostname(config)# password policy no-repeat-times 3 Hostname(config)# password policy strong

Verification	When you create a user and the corresponding password after configuring the password security policy, the system will perform relevant detection according to the password security policy. ● Run the **show password policy** command to display user-configured password security policy information.
	Hostname# show password policy Global password policy configurations: Password encryption: Enabled Password strong-check: Enabled Password min-size: Enabled (8 characters) Password life-cycle: Enabled (90 days) Password no-repeat-times: Enabled (max history record: 3)

Common Errors

- The time configured for giving a pre-warning notice about password expiry to the user is greater than the password life cycle.

1.4 Monitoring

Displaying

Description	Command
Displays user-configured password security policy information.	**show password policy**

1 Configuring SSH

1.1 Overview

Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is encrypted. When a user in an insecure network environment logs into a device remotely, SSH helps ensure information security and powerful authentication, protecting the device against attacks such as IP address spoofing and plain-text password interception.

An SSH-capable device can be connected to multiple SSH clients. In addition, the device can also function as an SSH client, and allows users to set up an SSH connection with a SSH-server device. In this way, the local device can safely log in to a remote device through SSH to implement management.

Currently, a device can work as either the SSH server or an SSH client, supporting SSHv1 and SSHv2 versions. The device supports SSH services of both IPv4 and IPv6.

Unless otherwise specified, SSH in this document refers to SSHv2.

Protocols and Standards

- RFC 4251: The Secure Shell (SSH) Protocol Architecture
- RFC 4252: The Secure Shell (SSH) Authentication Protocol
- RFC 4253: The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254: The Secure Shell (SSH) Connection Protocol
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716: The Secure Shell (SSH) Public Key File Format
- RFC 4819: Secure Shell Public Key Subsystem
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 1950: ZLIB Compressed Data Format Specification version 3.3
- draft-ietf-secsh-filexfer-05: SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00: The version of the SSH Remote Login Protocol is 1.5. Comware implements the SSH server functions, but not the SSH client functions.

1.2 Applications

Application	Description
SSH Device Management	Use SSH to manage devices.
SSH Local Line AuthenticationSSH Local Line Authentication	Use the local line password authentication for SSH user authentication.
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH

Application	Description
	user authentication.
SSH Public Key Authentication	Use the public key authentication for SSH user authentication.
SSH File Transfer	Use the Secure Copy (SCP) commands on the client to exchange data with the SSH server.

1.2.1 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 14-1 shows the network topology.

Figure 1-1 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.

1.2.2 SSH Local Line Authentication

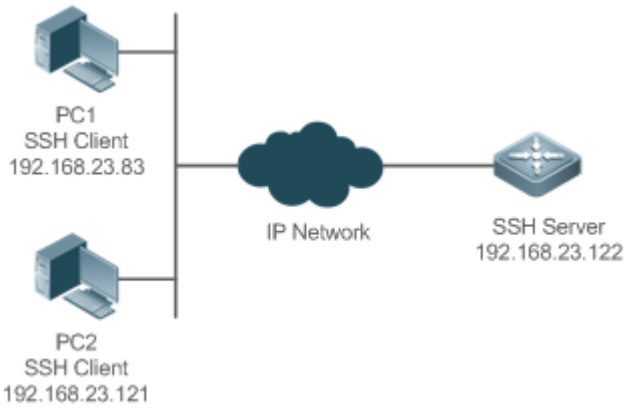
Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 14-2.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 1-2 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 FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server using this IP address. The routes from the SSH clients to the SSH server are reachable.

- Configure the SSH client as follows:

Diversified SSH client software is available, including PuTTY, Linux, and OpenSSH. This document takes PuTTY as an example to explain the method for configuring the SSH clients.

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".)

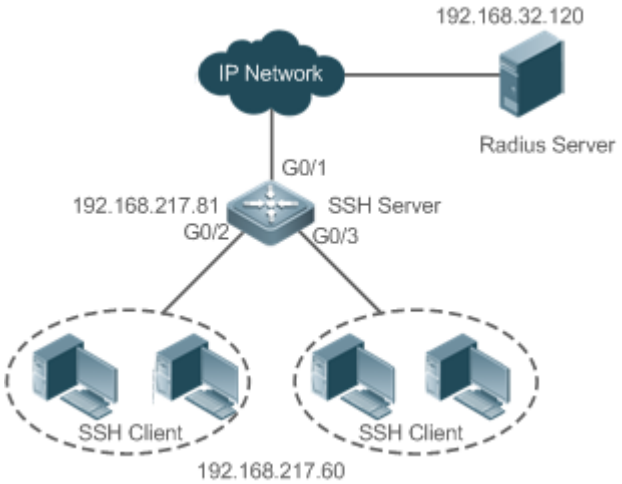
1.2.3 SSH AAA Authentication

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 14-3. To ensure security of data exchange, the PCs function as the SSH clients, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA

authentication mode is used for user login on the SSH clients. Two authentication methods, including RADIUS server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The RADIUS server authentication method is preferred. If the RADIUS server does not respond, it turns to the local authentication.

Figure 1-3 Networking Topology of SSH AAA Authentication



Deployment

- The routes from the SSH clients to the SSH server are reachable, and the route from the SSH server to the RADIUS server is also reachable.
- Configure the SSH server on the network device that functions as an SSH client.
- Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.

1.2.4 SSH Public Key Authentication

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 14-4. SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 1-4 Network Topology for Public Key Authentication of SSH Users



Deployment

- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure the public key on the SSH server, and select the public key authentication mode.

- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash and associates the file with the SSH user name. Each user can be associated with one RSA public key and one DSA public key.

1.2.5 SSH File Transfer

Scenario

The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server, as shown in Figure 14-5.

Figure 1-5 Networking Topology of SSH File Transfer



Deployment

- Enable the SCP service on the server.
- On the client, use SCP commands to upload files to the server, or download files from the server.

1.3 Features

Basic Concepts

User Authentication Mechanism

- Password authentication

During the password authentication, a client sends a user authentication request and encrypted user name and password to the server. The server decrypts the received information, compares the decrypted information with those stored on the server, and then returns a message indicating the successful or unsuccessful authentication.

- Public key authentication

During the public key authentication, digital signature algorithms, such as RSA and DSA, are used to authenticate a client. The client sends a public key authentication request to the server. This request contains information including the user name, public key, and public key algorithm. On receiving the request, the server checks whether the public key is correct. If wrong, the server directly sends an authentication failure message. If right, the server performs digital signature authentication on the client, and returns a message indicating the successful or unsuccessful authentication.

Public key authentication is applicable only to the SSHv2 clients.

SSH Communication

To ensure secure communication, interaction between an SSH server and an SSH client undergoes the following seven stages:

- Connection setup

The server listens on Port 22 to the connection request from the client. After originating a socket initial connection request, the client sets up a TCP socket connection with the server.

- Version negotiation

If the connection is set up successfully, the server sends a version negotiation packet to the client. On receiving the packet, the client analyzes the packet and returns a selected protocol version to the server. The server analyzes the received information to determine whether version negotiation is successful.

- Key exchange and algorithm negotiation

If version negotiation is successful, key exchange and the algorithm negotiation are performed. The server and the client exchange the algorithm negotiation packet with each other, and determine the final algorithm based on their capacity. In addition, the server and the client work together to generate a session key and a session ID according to the key exchange algorithm and host key, which will be applied to subsequent user authentication, data encryption, and data decryption.

- User authentication

After the encrypted channel is set up, the client sends an authentication request to the server. The server repeatedly conducts authentication for the client until the authentication succeeds or the server shuts down the connection because the maximum number of authentication attempts is reached.

- Session request

After the successful authentication, the client sends a session request to the server. The server waits and processes the client request. After the session request is successfully processed, SSH enters the session interaction stage.

- Session interaction

After the session request is successfully processed, SSH enters the session interaction stage. Encrypted data can be transmitted and processed in both directions. The client sends a command to be executed to the client. The server decrypts, analyzes, and processes the received command, and then sends the encrypted execution result to the client. The client decrypts the execution result.

- Session ending

When the interaction between the server and the client is terminated, the socket connection disconnects, and the session ends.

Overview

Feature	Description
SSH Server	Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client.
SCP Service	After the SCP service is enabled, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

1.3.1 SSH Server

Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client. You can also shut down the SSH server function to disconnect from all SSH clients.

Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts." In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

- Version: Configure the SSH version as SSHv1 orSSHv2 to connect SSH clients.
- Authentication timeout: The SSH server starts the timer after receiving a user connection request. The SSH server is disconnected from the client either when the authentication succeeds or when the authentication timeout is reached.
- Maximum number of authentication retries: The SSH server starts authenticating the client after receiving its connection request. If authentication does not succeed when the maximum number of user authentication retries is reached, a message is sent, indicating the authentication failure.
- Public key authentication: The public key algorithm can be RSA or DSA. It provides a secure connection between the client and the server. The public key file on the client is associated with the user name. In addition, the public key authentication mode is configured on the client, and the corresponding private key file is specified. In this way, when the client attempts to log in to the server, public key authentication can be implemented to set up a secure connection.

Related Configuration

↘ Enabling the SSH Server

By default, the SSH server is disabled.

In global configuration mode, run the [**no**] **enable service ssh-server** command to enable or disable the SSH server.

To generate the SSH key, you also need to enable the SSH server.

↘ Specifying the SSH Version

By default, the SSH server supports both SSHv1 and SSHv2, connecting either SSHv1 clients or SSHv2 clients.

Run the **ip ssh version** command to configure the SSH version supported by the SSH server.

If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

↘ Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

Run the **ip ssh time-out** command to configure the user authentication timeout of the SSH server. Use the **no** form of the command to restore the default timeout. The SSH server starts the timer after receiving a user

connection request. If authentication does not succeed before the timeout is reached, authentication times out and fails.

Configuring the Maximum Number of SSH Authentication Retries

By default, the maximum number of user authentication retries is 3.

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user authentication retries. If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

Configuring an Encryption Mode on the SSH Server

By default, the encryption mode on the SSH server is compatible (**cbc**, **ctr**, and **others**).

Run the **ip ssh cipher-mode** command to configure the encryption mode on the SSH server. Use the no form of the command to restore the default encryption mode on the SSH server.

Configuring a Message Authentication Algorithm on the SSH Server

By default, the SSHv1 server does not support message authentication algorithms, and the SSHv2 server supports MD5, SHA1, SHA1-96, and MD5-96.

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithm supported by SSH Server. Use the no form of the command to restore the default message authentication algorithm on the SSH server.

Configuring a DH Key Exchange Algorithm on the SSH Server

By default, the SSHv1 server does not support DH key exchange algorithms, and the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1.

Run the **ip ssh key-exchange** command to configure DH key exchange algorithms on the SSH server. Use the no form of the command to restore the default DH key exchange algorithms on the SSH server.

Configuring the Listening Port of the SSH Server

By default, the listening port of the SSH server is port 22.

Run the **ip ssh port** command to configure the listening port number of the SSH server. Use the no form of the command or run the **ip ssh port 22** command to restore the default listening port number of the SSH server..

Configuring an ACL for the SSH Server

By default, an ACL does not filter traffic of all connections on the SSH server.

Run the {**ip**| **ipv6** } **ssh access-class** command to configure an ACL to filter traffic of all connections on the SSH server. Use the no form of the command to restore the default setting.

Enabling the Public Key Authentication on the SSH Server

Run the **ip ssh peer** command to associate the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

1.3.2 SCP Service

The SSH server provides the SCP service to implement secure file transfer between the server and the client.

Working Principle

- SCP is a protocol that supports online file transfer. It runs on Port 22 based on the BSC RCP protocol, whereas RCP provides the encryption and authentication functions based on the SSH protocol. RCP implements file transfer, and SSH implements authentication and encryption.
- Assume that the SCP service is enabled on the server. When you use an SCP client to upload or download files, the SCP client first analyzes the command parameters, sets up a connection with a remote server, and starts another SCP process based on this connection. This process may run in source or sink mode. (The process running in source mode is the data provider. The process running in sink mode is the destination of data.) The process running in source mode reads and sends files to the peer end through the SSH connection. The process running in sink mode receives files through the SSH connection.

Related Configuration

Enabling the SCP Server

By default, the SCP server function is disabled.

Run the **ip scp server enable** command to enable SCP server function on a network device.

1.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	⚠ It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.
	disconnect ssh[**vty**] *session-id*	Disconnects an established SSH session.
	crypto key generate {**rsa**|**dsa**}	Generates an SSH key.
	crypto key zeroize { **dsa** | **rsa** }	Deletes 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** }	Configures an encryption mode on the SSH server.
	ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** }	Configures a message authentication algorithm on the SSH server.
	ip ssh key-exchange { **dh_group_exchange_sha1** | **dh_group1_sha1** | **dh_group14_sha1** }	Configures DH key exchange algorithms on the SSH server.

Configuration	Description and Command	
	ip ssh port	Configures the listening port of the SSH server.
	{**ip**| **ipv6** } **ssh access-class** { *access-list-number* | *access-list-name* }	Configures an ACL for the SSH server.
	ip ssh peer *test* **public-key rsa flash** *:rsa.pub*	Associates an RSA public key file with a user.
	ip ssh peer *test* **public-key dsa flash***:dsa.pub*	Associates a DSA public key file with a user.
Configuring the SCP Service	⚠ Mandatory.	
	ip scp server enable	Enables the SCP server.

1.4.1 Configuring the SSH Server

Configuration Effect

- Enable the SSH server function on a network device so that you can set up a secure connection with a remote network device through the SSH client. All interactive data is encrypted before transmitted, featuring authentication and security.
- You can use diversified SSH user authentications modes, including local line password authentication, AAA authentication, and public key authentication.
- You can generate or delete an SSH key.
- You can specify the SSH version.
- You can configure the SSH authentication timeout.
- You can configure the maximum number of SSH authentication retries.
- You can configure an encryption mode on the SSH server.
- You can configure a message authentication algorithm on the SSH server.
- You can configure an ACL for the SSH server.

Notes

- The precondition of configuring a device as the SSH server is that communication is smooth on the network that the device resides, and the administrator can access the device management interface to configure related parameters.
- The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key.

Configuration Steps

↘ Enabling the SSH Server

- Mandatory.

- By default, the SSH server is disabled. In global configuration mode, enable the SSH server and generate an SSH key so that the SSH server state changes to ENABLE.

Specifying the SSH Version

- Optional.
- By default, the SSH server supports SSHv1 and SSHv2, connecting either SSHv1 or SSHv2clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

Configuring the SSH Authentication Timeout

- Optional.
- By default, the SSH authentication timeout is 120s. You can configure the user authentication timeout as required. The value ranges from 1 to 120. The unit is second.

Configuring the Maximum Number of SSH Authentication Retries

- Optional.

  Configure the maximum number of SSH authentication retries to prevent illegal behaviors such as malicious guessing. By default, the maximum number of SSH authentication retries is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum number of retries as required. The value ranges from 0 to 5.

Configuring an Encryption Mode on the SSH Server

- Optional.
- Configure an encryption mode on the SSH server. By default, the encryption mode on the SSH server is compatible (**cbc**, **ctr**, and **others**).

Configuring a Message Authentication Algorithm on the SSH Server

- Optional.
- Configure a message authentication algorithm on the SSH server. By default, the SSHv1 server does not support message authentication algorithms, and the SSHv2 server supports MD5, SHA1, SHA1-96, and MD5-96.

Configuring an ACL for the SSH Server

- Optional.
- Configure an ACL for the SSH server. By default, an ACL is not used to filter traffic of all connections of the SSH server. You can configure an ACL to filter traffic of all connections of the SSH server.

Enabling the Public Key Authentication for SSH Users

- Optional.
- Only SSHv2 supports authentication based on the public key. This configuration associates a public key file on the client with a user name. When a client is authenticated upon login, a public key file is specified based on the user name.

Verification

- Run the **show ip ssh** command to display the current SSH version, port number, encryption mode, message 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
Usage Guide	The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. If an RSA key is generated, both SSHv1 and SSHv2 are supported. If only a DSA key is generated, only SSHv2 can use the key.

Deleting a Key

Command	**crypto key zeroize** { **dsa** | **rsa** }
Parameter Description	**dsa**: deletes a DSA key. **rsa**: deletes an RSA key.
Command Mode	Global configuration mode
Usage Guide	This command is used to delete the public key of the SSH server. After the public key is deleted, the SSH server status is **DISABLE**. To disable the SSH server, use the no form of this command..

Specifying the SSH Version

Command	**ip ssh version** {**1**|**2**}
Parameter Description	**1**: indicates that the SSH server only receives the connection requests sent by SSHv1 clients. **2**: indicates that the SSH server only receives the connection requests sent by SSHv2 clients.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh version** command to restore the default settings. By default, the SSH server supports both SSHv1 and SSHv2.

Configuring the SSH Authentication Timeout

Command	**ip ssh time-out** *time*
Parameter Description	*time*: indicates the SSH authentication timeout. The value ranges from 1 to 120. The unit is second.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh time-out** command to restore the default SSH authentication timeout, which is 120s.

Configuring the Maximum Number of SSH Authentication Retries

Command	**ip ssh authentication-retries** *retry-times*
Parameter Description	*retry-times*: indicates the maximum number of user authentication retries. The value ranges from 0 to 5.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh authentication-retries** command to restore the default number of user authentication retries, which is 3.

Configuring an Encryption Mode on the SSH Server

Command	**ip ssh cipher-mode** { **cbc** | **ctr** | **others**}
Parameter Description	**cbc**: configures the encryption mode as cipher block chaining (CBC) on the SSH server. The corresponding encryption algorithms are DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, and Blowfish-CBC. **ctr**: configures the encryption mode as counter mode (CTR) on the SSH server. The corresponding encryption algorithms are AES128-CTR, AES192-CTR, and AES256-CTR. **others**: configures the encryption mode as others. The corresponding encryption algorithm is RC4.

Command Mode	Global configuration mode
Usage Guide	Run the **ip ssh cipher-mode** command to configure an encryption mode on the SSH server. The SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES- 128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. These algorithms can be grouped into three types of encryption modes: CBC, CTR, and others. As the cryptography continuously develops, encryption algorithms in CBC and others modes are proved to be decrypted in a limited period of time. Therefore, organizations or companies that require high security can set the encryption modes on the SSH server to CTR to enhance the security of the SSH server.

Configuring a Message Authentication Algorithm on the SSH Server

Command	**ip ssh hmac-algorithm** { **md5** | **md5-96** | **sha1** | **sha1-96** }
Parameter Description	**md5**: sets the message authentication algorithm to MD5 on the SSH server. **md5-96**: sets the message authentication algorithm to MD5-96 on the SSH server. **sha1**: sets the message authentication algorithm to SHA1 on the SSH server. **sha1-96**: sets the message authentication algorithm to SHA1-96 on the SSH server.
Command Mode	Global configuration mode
Usage Guide	Run the **ip ssh hmac-algorithm** command to configure a message authentication algorithm on the SSH server. The SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, SHA1, SHA1-96, and MD5-96. You can select a message authentication algorithm supported by the SSH server as required.

Configuring a DH Key Exchange Algorithm on the SSH Server

Command	**ip ssh key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** }
Parameter Description	**dh_group_exchange_sha1**: sets the DH key exchange algorithm to diffie-hellman-group-exchange-sha1. The default key length is 2048 bytes and cannot be configured. **dh_group14_sha1**: sets the DH key exchange algorithm to diffie-hellman-group14-sha1. The key length ranges from 1 to 2048 bytes. **dh_group1_sha1**: sets the DH key exchange algorithm to diffie-hellman-group1-sha1. The key length is 1024 bytes.
Command Mode	Global configuration mode
Usage Guide	Run the **ip ssh key-exchange** command to configure a DH key exchange algorithm on the SSH server. By default, the SSHv1 server does not support DH key exchange algorithms, and the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1. You can select a DH key exchange algorithm on the SSH server as required.

Configuring the Listening Port of the SSH Server

Command	**ip ssh port** *port*
Parameter Description	*port*: configures the listening port number of the SSH server. The value range is 1025–65535.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh port** or **ip ssh port 22** command to restore the listening port number of the SSH server to port 22.

Configuring an ACL for the SSH Server

Command	{**ip**| **ipv6** } **ssh access-class** { *access-list-number*	*access-list-name* }
Parameter Description	*access-list-number*: specifies the ACL ID. The value range of IP standard ACLs is 1–99 or 1300–1999; the value range of IP extended ACLs is 100–199 or 2000–2699. *access-list-name*: specifies the ACL name. It is supported by IPv4 and IPv6.
Command Mode	Global configuration mode
Usage Guide	Run the **ssh access-class** command to configure an ACL to filter traffic of all connections of the SSH server. In line mode, an ACL is used to filter traffic on a specific line only. However, an ACL on the SSH server is used to filter traffic of all SSH connections.

Configuring RSA Public Key Authentication

Command	**ip ssh peer** *username* **public-key rsa** *filename*
Parameter Description	*username*: indicates the user name. **rsa**: indicates that the public key type is RSA. *filename*: indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	Run the **ip ssh peer** command to configure the RSA public key file associated with user. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Configuring DSA Public Key Authentication

Command	**ip ssh peer** *username* **public-key dsa** *filename*
Parameter Description	*username*: indicates the user name. **dsa**: indicates that the public key type is DSA. *filename*: indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	Run the **ip ssh peer** command to configure the DSA key file associated with user. 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.

Configuration Example

The following configuration examples describe only configurations related to SSH.

Generating a Public Key on the SSH Server

Configuration Steps	● Run the **crypto key generate { rsa | dsa }** command to generate a RSA public key for the server.
SSH Server	Hostname#configure terminal Hostname(config)# crypto key generate rsa Choose the size of the rsa key modulus in the range of 512 to 2048 and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: ● If the generation of the RSA key is successful, the following information is displayed: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] ● If the generation of the RSA key fails, the following information is displayed: % Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]
Verification	● Run the **show crypto key mypubkey rsa** command to display the public information about the RSA key. If the public information about the RSA key exists, the RSA key has been generated.
SSH Server	Hostname(config)#show crypto key mypubkey rsa % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU 8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t 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 F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISgIfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEYXCFaaxU=

Specifying the SSH Version

Configuration Steps	● Run the **ip ssh version** { **1** | **2** } command to set the version supported by the SSH server to SSHv2.
SSH Server	Hostname#configure terminal Hostname(config)#ip ssh version 2
Verification	● Run the **show ip ssh** command to display the SSH version currently supported by the SSH server.
SSH Server	Hostname#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,sha2-256,sha2-512 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the SSH Authentication Timeout

Configuration Steps	● Run the **ip ssh time-out** *time* command to set the SSH authentication timeout to 100s.
SSH Server	Hostname#configure terminal Hostname(config)#ip sshtime-out100
Verification	● Run the **show ip ssh** command to display the configured SSH authentication timeout.
SSH Server	Hostname#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,sha2-256,sha2-512 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the Maximum Number of SSH Authentication Retries

Configuration Steps	● Run the **ip ssh authentication-retries** *retry times* command to set the maximum number of user authentication retries on the SSH server to 2.
SSH Server	Hostname#configure terminal Hostname(config)#ip ssh authentication-retries 2
Verification	● Run the **show ip ssh** command to display the configured maximum number of authentication retries.
SSH Server	Hostname#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,sha2-256,sha2-512 Authentication timeout: 120 secs Authentication retries: 2 SSH SCP Server: disabled

Configuring an Encryption Mode on the SSH Server

Configuration Steps	● Run the **ip ssh cipher-mode** { **cbc** | **ctr** | **others** } command to configure an encryption mode on the SSH server. The CTR encryption mode is used as an example.
SSH Server	Hostname# configure terminal Hostname(config)# ip ssh cipher-mode ctr
Verification	● Select the CTR encryption mode on the SSH client to check whether the SSH client can log in.

Configuring a Message Authentication Algorithm on the SSH Server

Configuration	● Run the **ip ssh hmac-algorithm** { **md5** | **md5-96** | **sha1** | **sha1-96** } command to configure a message authentication algorithm on the SSH server. SHA1 is used as an example.
SSH Server	Hostname# configure terminal Hostname(config)# ip- sha1
Verification	● Select SHA1 on the SSH client to check whether the SSH client can log in.

Configuring a DH Key Exchange Algorithm on the SSH Server

Configuration Steps	● Run the **ip ssh key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** } command to configure a DH key exchange algorithm on the SSH server. diffie-hellman-group14-sha1 is used as an example.
SSH Server	Hostname# configure terminal Hostname(config)# ip ssh key-exchange dh_group14_sha1
Verification	● Select diffie-hellman-group14-sha1 on the SSH client to check whether the SSH client can log in.

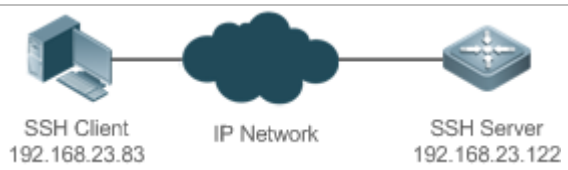
Configuring the Listening Port of the SSH Server

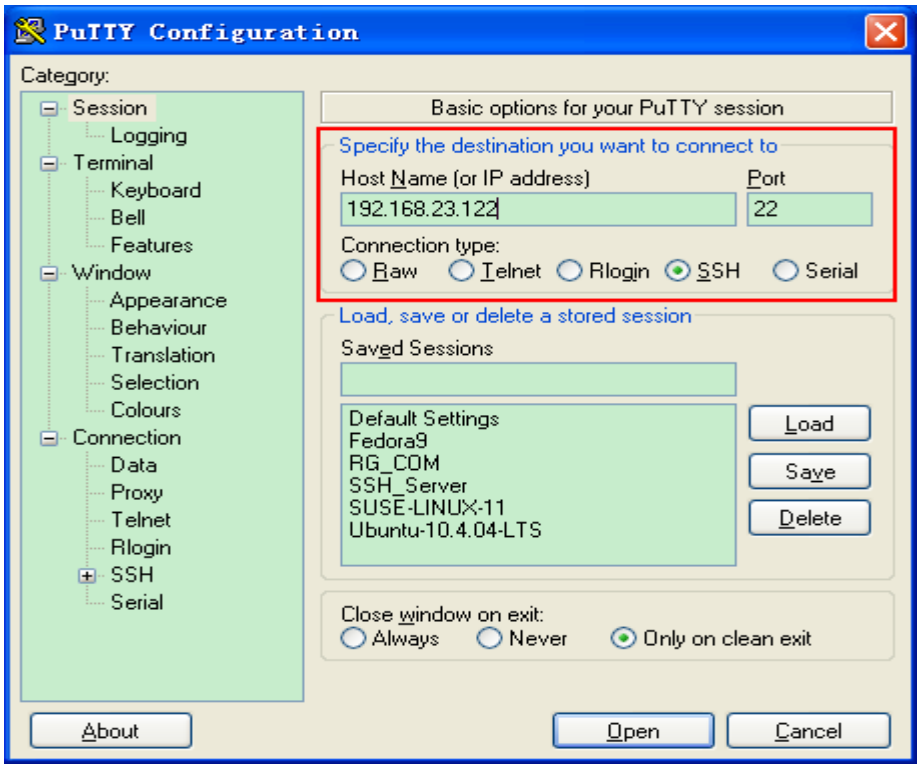
Configuration Steps	● Run the **ip ssh port** *port* command to configure the listening port number of the SSH server. Port 10000 is used as an example.
SSH Server	Hostname# configure terminal Hostname(config)# ip ssh port 10000
Verification	● Run the **show ip ssh** command to check information about the listening port number of the SSH server. Hostname# show run SSH Enable - version 2.0 Port 10000 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1,sha2-256,sha2-512 Authentication & Accounting 120 secs Authentication retries: 3 SSH SCP Server: wis disabled.

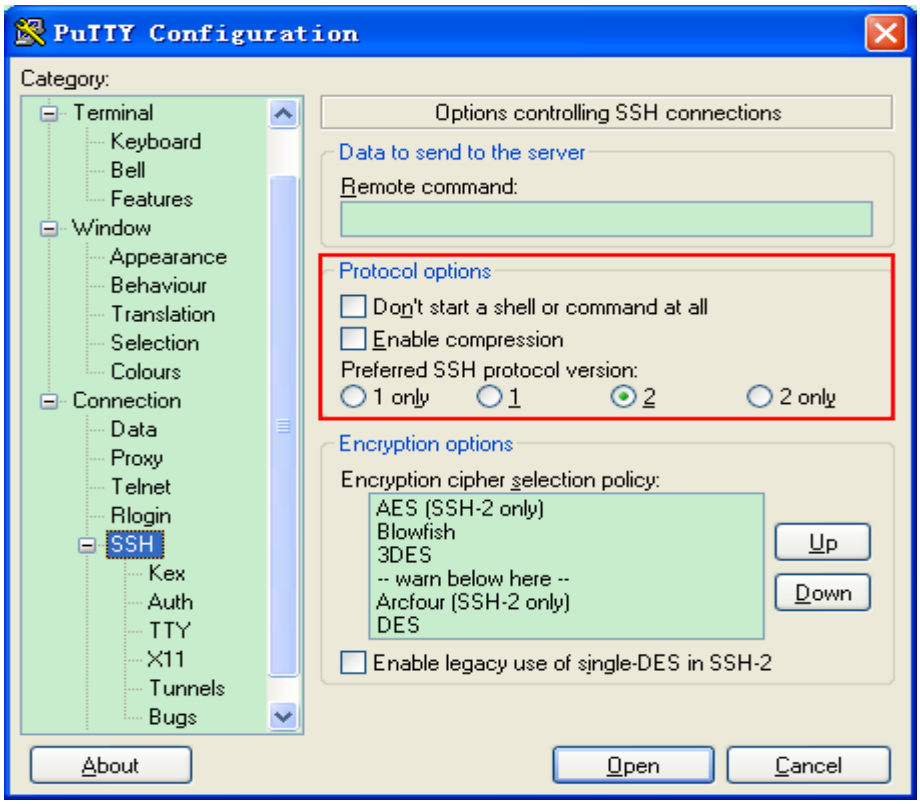
Configuring the Public Key Authentication

Configuration Steps	● Run the **ip ssh peer** *username* **public-key** { **rsa** | **dsa**}*filename* command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA) is specified based on the user name.
SSH Server	Hostname#configure terminal Hostname(config)# ip ssh peer test public-key rsaflash:rsa.pub
Verification	● Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Configuring SSH Device Management

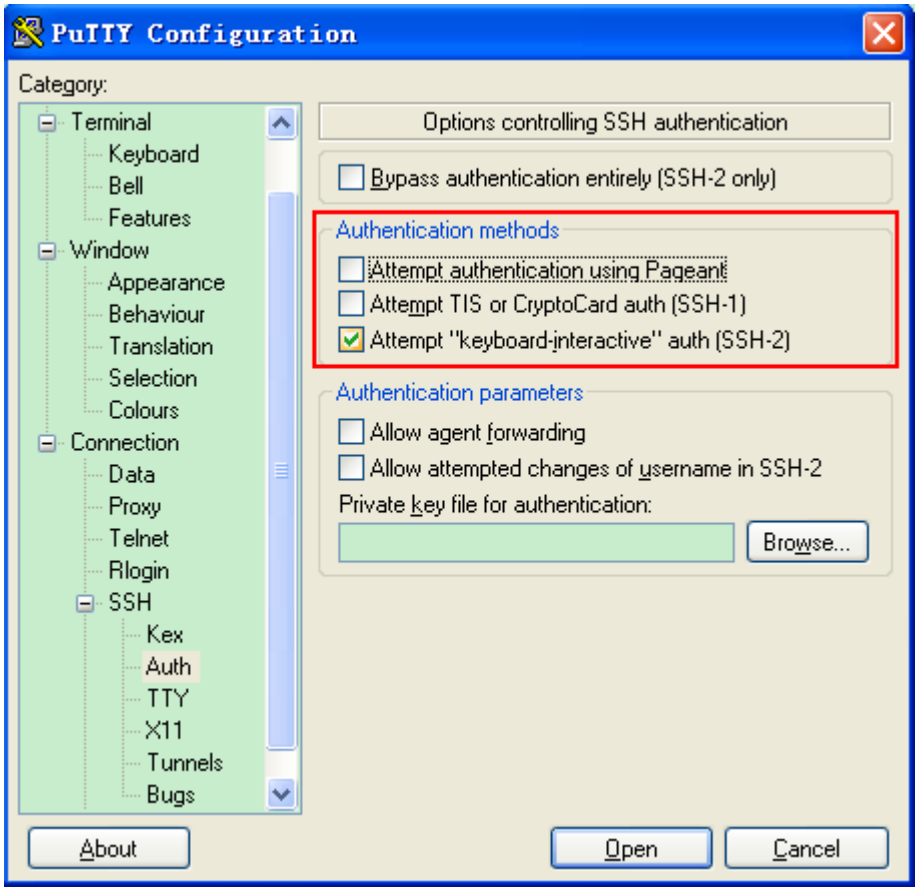
Scenario Figure 1-6	

	You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible client software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.
Configuration Steps	● Start the PuTTY software. ● On the **Session** option tab of PuTTY, type in the host IP address **192.168.23.122** and SSH port number **22**, and select the connection type **SSH**. ● On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**. ● On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**. ● Click **Open** to connect to the SSH server. ● Type in the correct user name and password to enter the terminal login interface.
SSH Client	Figure 1-7  **Host Name (or IP address)** indicates the IP address of the host to be logged in. In this example, the IP address is **192.168.23.122**. **Port** indicates the port ID 22, that is, the default ID of the port listened by SSH. **Connection type** is **SSH**. Figure 1-8



As shown in Figure 14-8, select **2** as the preferred SSH protocol version in the **Protocol options** pane because SSHv2 is used for login.

Figure 1-9



As shown in Figure 14-9, select **Attempt "keyboard-interactive" auth** as the authentication method to support authentication based on the user name and password.

Then, click **Open** to connect to the configured server host, as shown in Figure 14-9.

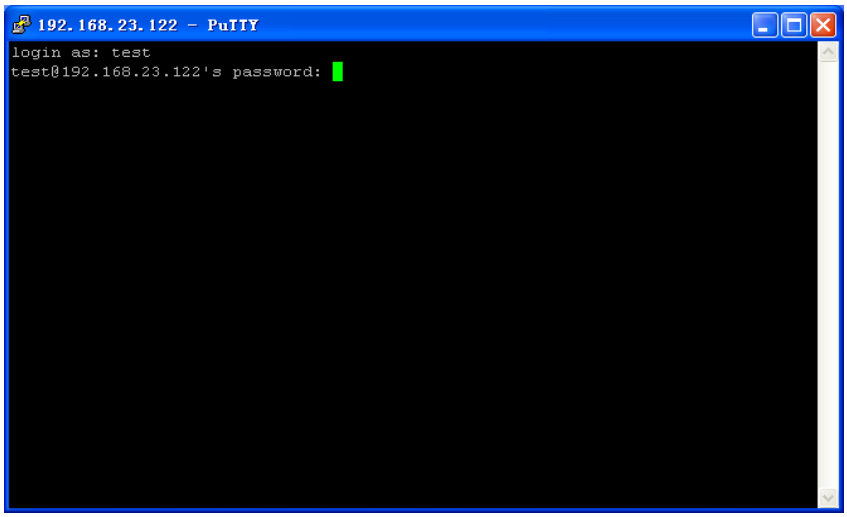
Figure 1-10



The **PuTTY Security Alert** box indicates that you are logging in to the client of the server 192.168.23.122, and asks you whether to receive the key sent from the server.

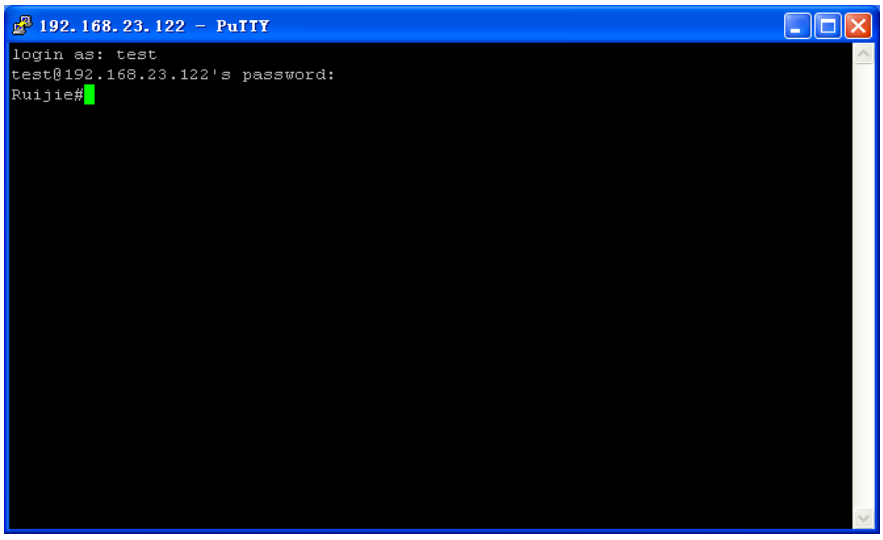
If you select **Yes**, a login dialog box is displayed, as shown in Figure 14-10.

Figure 1-11



Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 14-11.

Figure 1-12



Verification

- Run the **show ip ssh** command to display the configurations that are currently effective on the SSH server.
- Run the **show ssh** command to display information about every SSH connection that has been established.

```
Hostname#show ip ssh

SSH Enable - version 1.99

SSH Port:                       22
SSH Cipher Mode:                cbc,ctr,others
SSH HMAC Algorithm:             md5-96,md5,sha1-96,sha1,sha2-256,sha2-512

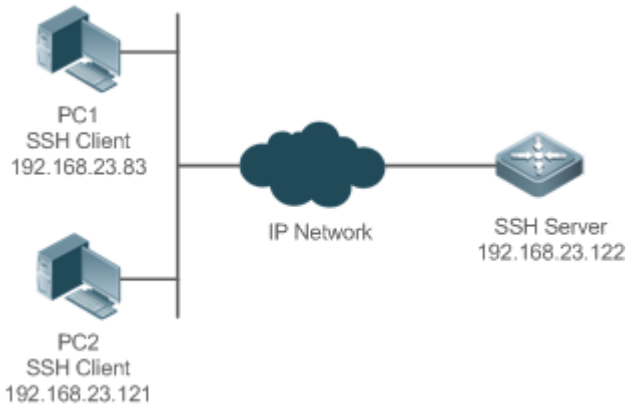
Authentication timeout: 120 secs

Authentication retries: 3

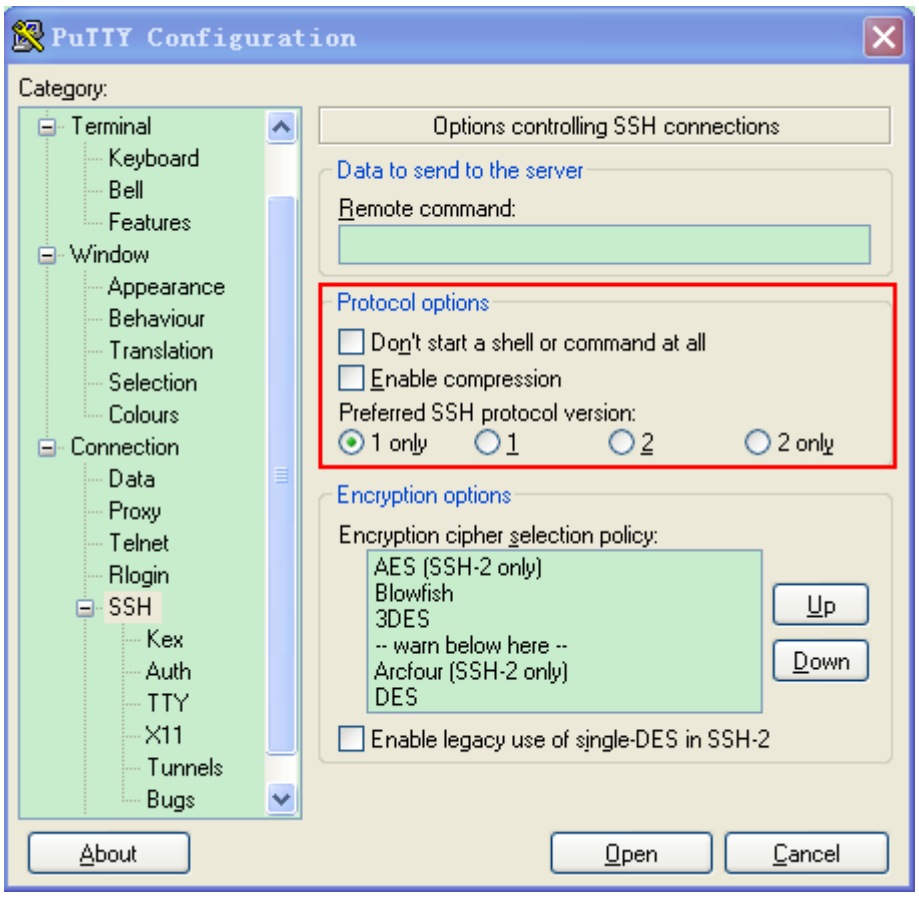
SSH SCP Server:                 disabled
```

	Hostname#show ssh Connection Version Encryption Hmac State Username 0 2.0 aes256-cbc hmac-sha1 Session started test

Configuring SSH Local Line Authentication

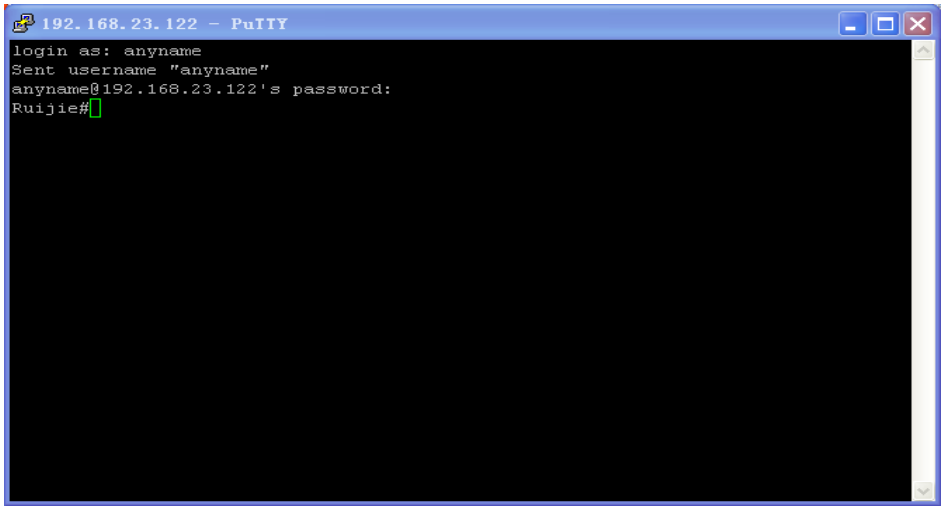
Scenario **Figure 1-13**	 SSH users can use the local line password for user authentication, as shown in Figure 15-12.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server is enabled. The requirements are as follows: ● SSH users use the local line password authentication mode. ● Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.
Configuration Steps	Configure the SSH server as follows: ● Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. ● Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ● Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH client to the SSH server is reachable. Configure the SSH client as follows: ● Diversified SSH client software is available, including PuTTY, Linux, and SecureCRT. This document takes PuTTY as an example to explain the method for configuring the SSH client. For details about the configuration method, see "Configuration Steps."
SSH Server	Before configuring SSH-related function, ensure that the route from the SSH user to the network segment of the SSH server is reachable. The interface IP address configurations are shown in Figure 15-12. The detailed procedures for configuring IP addresses and routes are omitted. Hostname(config)# enable service ssh-server

	Hostname(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet0/1)#ip address 192.168.23.122 255.255.255.0 Hostname(config-if-GigabitEthernet0/1)#exit Hostname(config)#line vty 0 Hostname(config-line)#password passzero Hostname(config-line)#privilege level 15 Hostname(config-line)#login Hostname(config-line)#exit Hostname(config)#line vty1 4 Hostname(config-line)#password pass Hostname(config-line)#privilege level 15 Hostname(config-line)#login Hostname(config-line)#exit
SSH Client(PC1/ PC2)	Figure 1-14

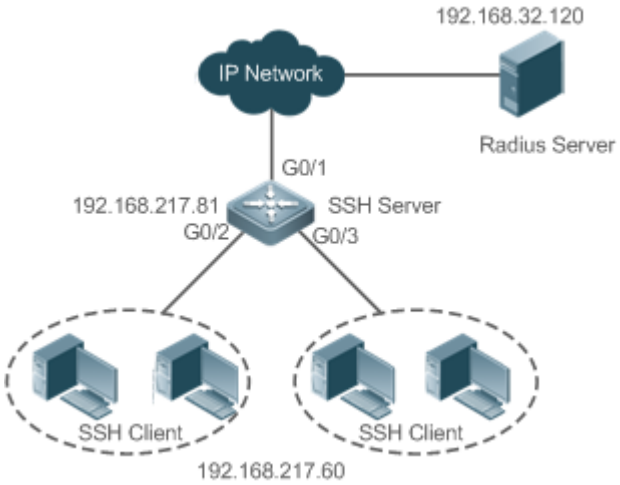


Set the IP address and port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22 (For details about the configuration method, see "Configuring SSH Device Management."). Click **Open** to start the SSH server. As the current authentication mode does not require a user name, you can type in any user name, but cannot leave the user name unspecified. (In this example, the user name is "anyname".)

Verification	● Run the **show running-config** command to display the current configurations. ● Verify that the SSH client configurations are correct.
SSH Server	Hostname#show running-config Building configuration... ! enable secret 5 1eyy2$xs28FDw4s2q0tx97 enable service ssh-server ! interface fastEthernet0/1 ip address 192.168.23.122 255.255.255.0 ! line vty 0 privilege level 15

	login password passzero line vty 1 4 privilege level 15 login password pass ! end
SSH Client	Set up a connection, and enter the correct password. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Then, the SSH server operation interface is displayed, as shown in Figure 15-14 Figure 1-15  Hostname#show users Line User Host(s) Idle Location ---------- ---------- ---------- ---------- ---------- * 0 con 0 --- idle 00:00:00 --- 1 vty 0 --- idle 00:08:02 192.168.23.83 2 vty 1 --- idle 00:00:58 192.168.23.121

Configuring AAA Authentication of SSH Users

Scenario **Figure 1-16**	 SSH users can use the AAA authentication mode for user authentication, as shown in Figure 15-15. To ensure security of data exchange, the PC functions as the SSH client, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods, including RADIUS server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The RADIUS server authentication method is preferred. If the RADIUS server does not respond, select the local authentication method.
Configuration Steps	● The route from the SSH client to the SSH server is reachable, and the route from the SSH server to the RADIUS server is also reachable. ● Configure the SSH server on the network device. The configuration method is already described in the previous example, and therefore omitted here. ● Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.
SSH Server	Hostname(config)# enable service ssh-server Hostname(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Hostname(config)#crypto key generate dsa

	Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit DSA keys ...[ok] Hostname(config)#interface gigabitEthernet1/1 Hostname(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0 Hostname(config-if-gigabitEthernet1/1)#exit Hostname#configure terminal Hostname(config)#aaa new-model Hostname(config)#radius-server host 192.168.32.120 Hostname(config)#radius-server key aaaradius Hostname(config)#aaa authentication login methodgroup radius local Hostname(config)#line vty 0 4 Hostname(config-line)#login authentication method Hostname(config-line)#exit Hostname(config)#username user1 privilege 1 password 111 Hostname(config)#username user2 privilege 10 password 222 Hostname(config)#username user3 privilege 15 password 333 Hostname(config)#enable secret w
Verification	● Run the **show running-config** command to display the current configurations. ● This example assumes that the SAM server is used. ● Set up a remote SSH connection on the PC. ● Check the login user.
	Hostname#show run aaa new-model ! aaa authentication login method group radius local ! username user1 password 111 username user2 password 222 username user2 privilege 10 username user3 password 333 username user3 privilege 15

```
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet1/1
 no ip proxy-arp
ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
End
```

On the SSH client, choose **System Management**>**Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**.

Choose **Security Management**>**Device Management Rights**, and set the rights of the login user.

Choose **Security Management**>**Device Administrator**, and add the user name **user** and password **pass**.

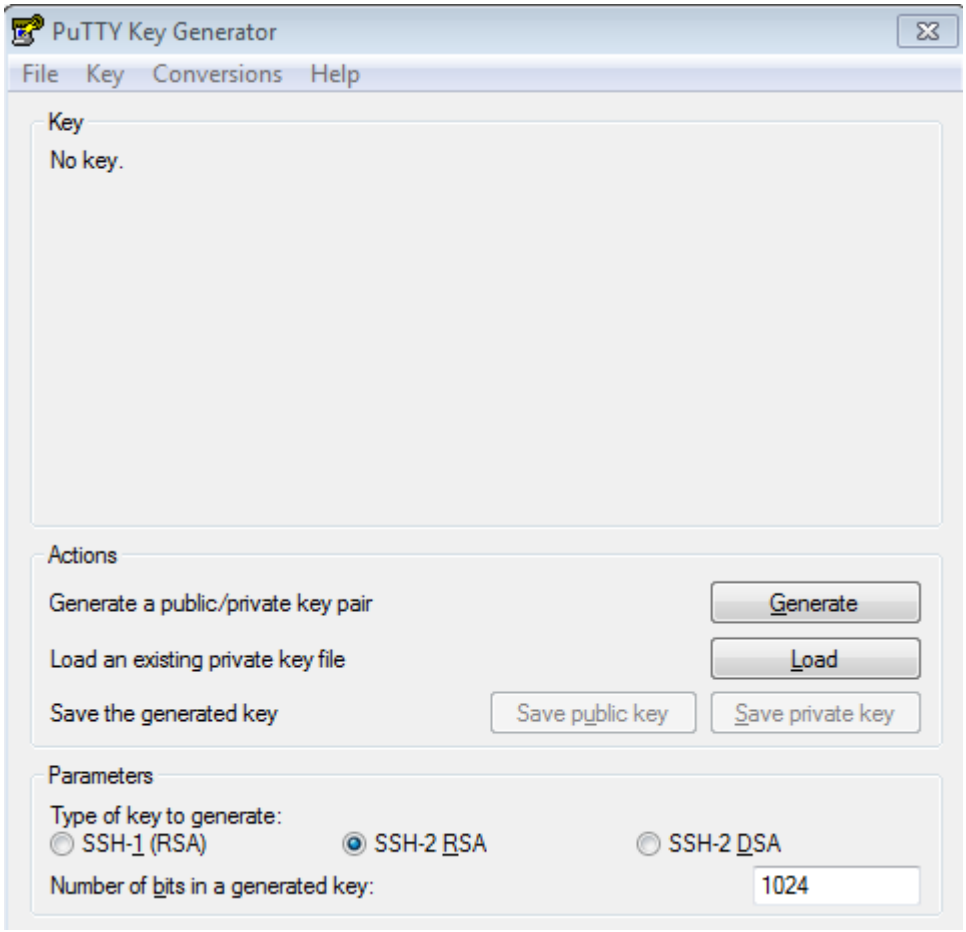
Configure the SSH client and set up a connection to the SSH server. For details, see the previous example.

Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
Hostname#show users
    Line          User          Host(s)              Idle         Location
   0 con 0                     idle                 00:00:31
* 1 vty 0       user          idle                 00:00:33     192.168.217.60
```

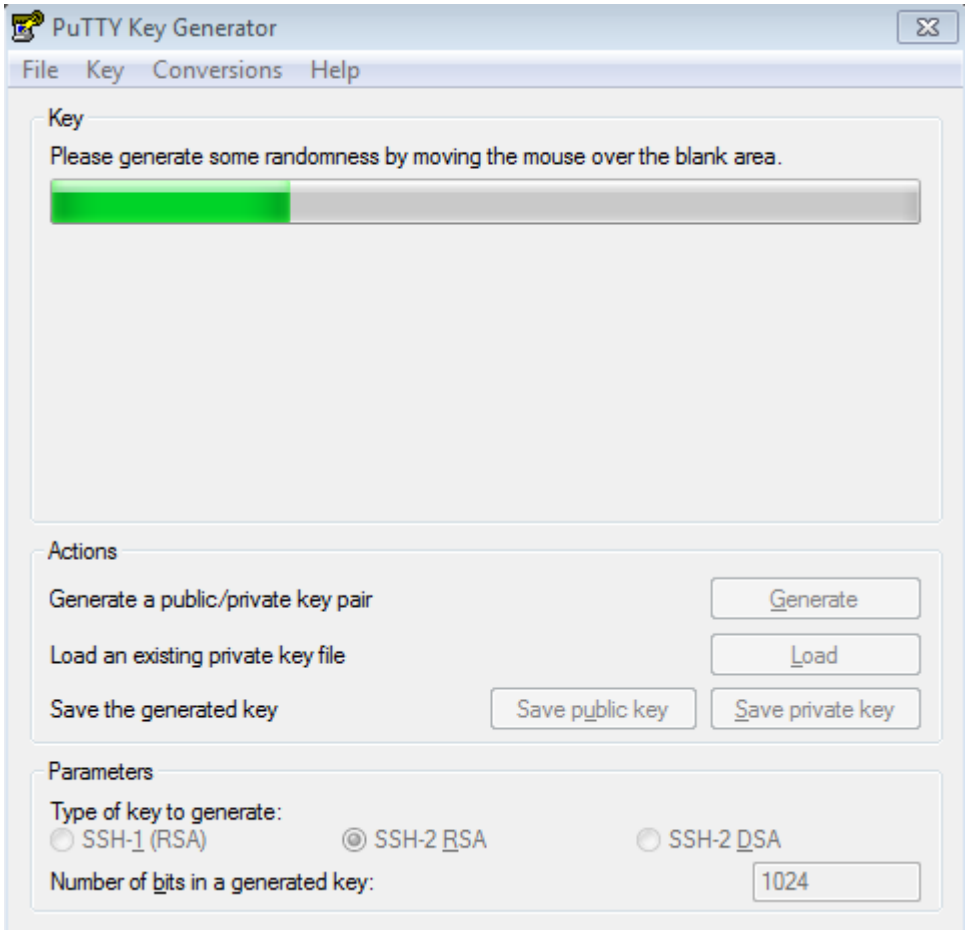
Configuring Public Key Authentication of SSH Users

Scenario Figure 1-17	 SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 15-16.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.
Configuration Steps	● To implement public key authentication on the client, generate a key pair (for example, RSA key) on the client, place the public key on the SSH server, and select the public key authentication mode. After the key pair is generated on the client, you must save and upload the public key file to the server and complete the server-related settings before you can continue to configure the client and connect the client with the server. ● After the key is generated on the client, copy the public key file from the client to the flash of the SSH server, and associate the file with an SSH user name. A user can be associated with one RSA public key and one DSA public key.
SSH Client	Run the **puttygen.exe** software on the client. Select **SSH-2 RSA** in the **Parameters** pane, and click **Generate** to generate a key, as shown in Figure 14-18. Figure 1-18



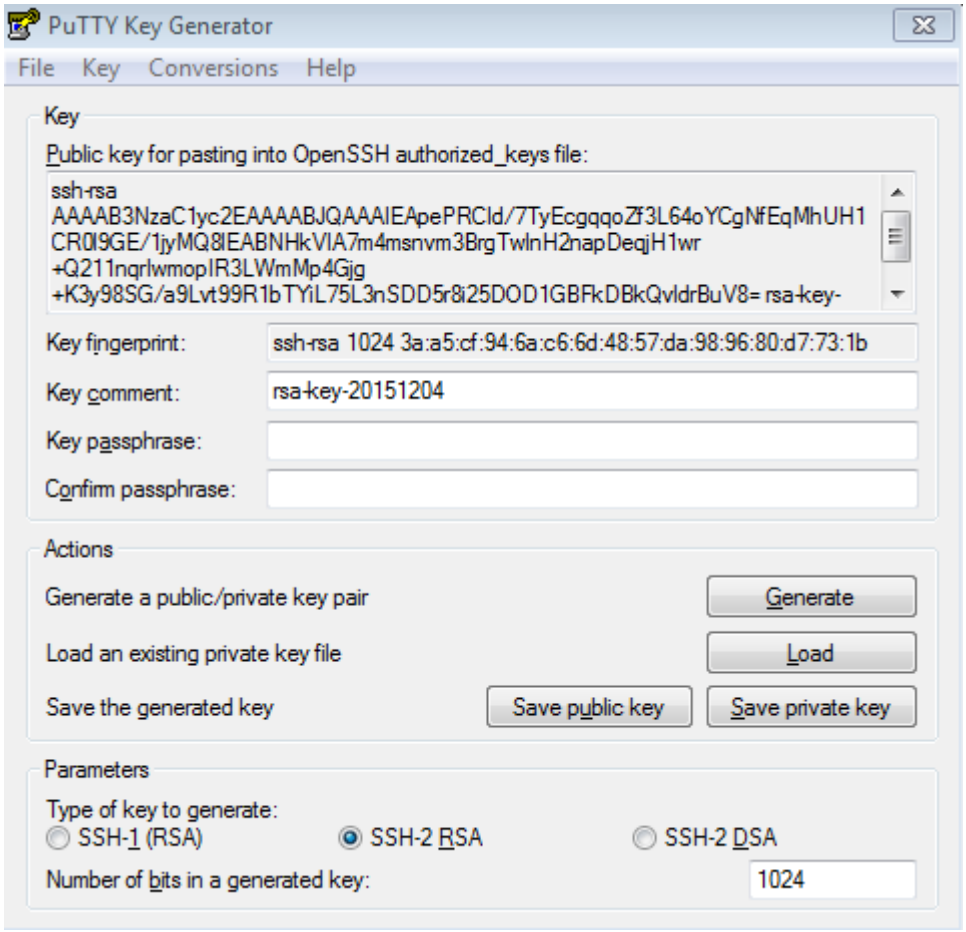
When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 14-19.

Figure 1-19



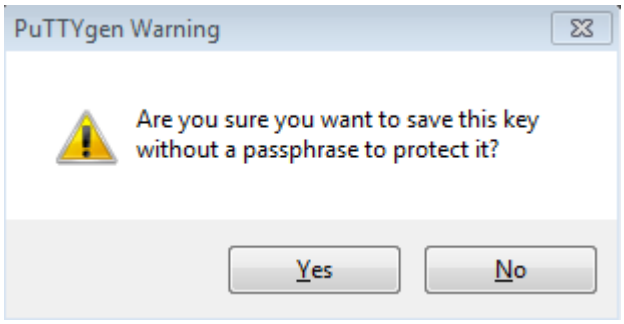
To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 1-20



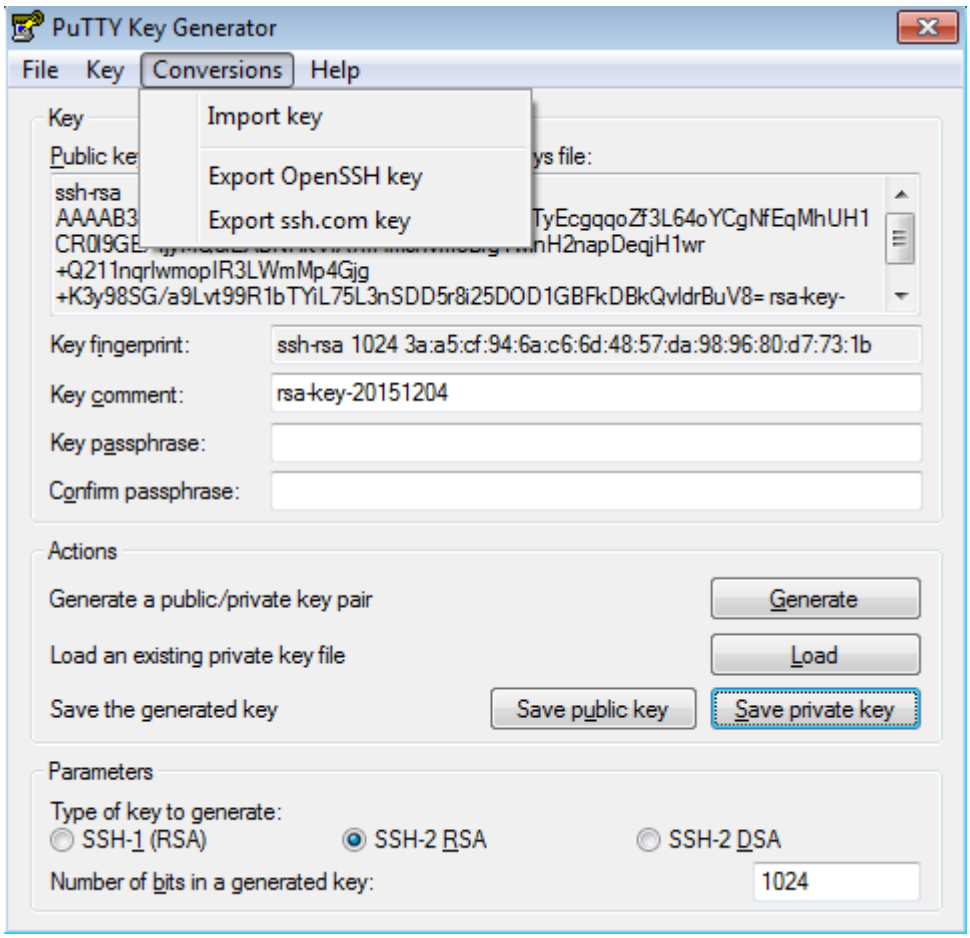
After the key pair is generated, click **Save public key**, type in the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following prompt box is displayed. Select **Yes**, type in the public key name **test_private**, and click **Save**.

Figure 1-21

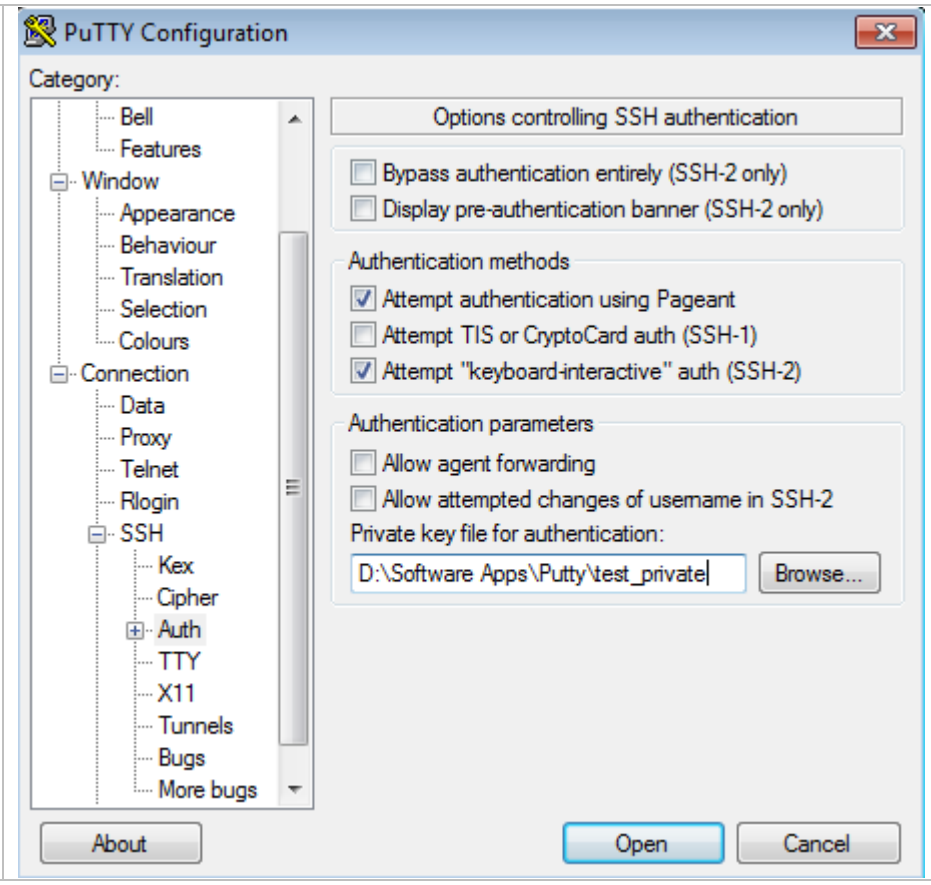


You must select the OpenSSH key file; otherwise, the key file cannot be used. The **puttygen.exe** software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. Format conversion is not required for the public key file stored on the server, and the format of this file is still OpenSSH, as shown in Figure 14-22.

Figure 1-22



SSH Server	Hostname#configure terminal Hostname(config)# ip ssh peer test public-key rsaflash:test_key.pub
Verification	● After completing the basic configurations of the client and the server, specify the private key file **test_private** on the PuTTY client, and set the host IP address to **192.168.23.122** and port ID to **22** to set up a connection between the client and the server. In this way, the client can use the public key authentication mode to log in to the network device.
	Figure 1-23



Common Errors

- The **no crypto key generate** command is used to delete a key.

1.4.2 Configuring the SCP Service

Configuration Effect

After the SCP function is enabled on a network device, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

Notes

- The SSH server must be enabled in advance.

Configuration Steps

↘ Enabling the SCP Server

- Mandatory.
- By default, the SCP server function is disabled. Run the **ip scp server enable** command to enable the SCP server function in global configuration mode.

Verification

Run the **show ip ssh** command to check whether the SCP server function is enabled.

Related Commands

↘ Enabling the SCP Server

Command	**ip scp server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to enable the SCP server. Run the **no ip scp server enable** command to disable the SCP server.

Configuration Example

↘ Enabling the SCP Server

Configuration Steps	● Run the **ip scp server enable** command to enable the SCP server.
	Hostname#configure terminal Hostname(config)#ip scp server enable
Verification	● Run the **show ip ssh** command to check whether the SCP server function is enabled.
	Hostname(config)#show 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,sha2-256,sha2-512 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled

↘ Configuring SSH File Transfer

Scenario Figure 1-24	 The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.
Configuration Steps	● Enable the SCP service on the server.

	The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can finds out that the user type is SSH by running the show user command). ● On the client, use SCP commands to upload files to the server, or download files from the server. Syntax of the SCP command: scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 [...] [[user@]host2:]file2 Descriptions of some options: -1: Uses SSHv1 (If not specified, SSHv2 is used by default); -2: Uses SSHv2 (by default); -C: Uses compressed transmission. -c: Specifies the encryption algorithm to be used. -r:Transmits the whole directory; -i: Specifies the key file to be used. -l: Limits the transmission speed (unit: Kbit/s). For other parameters, see the filescp.0. Most options are related to terminals. Few options are supported on both terminals and servers. SCP servers do not support d-p-q-r options. When these options are applied, there are prompts.
SSH Server	Hostname#configure terminal Hostname(config)# ip scp server enable
Verification	● File transmission example on the Ubuntu 7.10 system: Set the username of a client to **test** and copy the **config.text** file from the network device with the IP address of 192.168.195.188 to the **/root** directory on the local device.
	root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text 100% 1506 1.5KB/s 00:00 Read from remote host 192.168.195.188: Connection reset by peer

1.5 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**
Debugs sessions of the SSH client.	**debug ssh client**

Configuring Reliability

1. Configuring RLDP

1 Configuring RLDP

1.1 Overview

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid incorrect forwarding of traffic or Ethernet L2 loops.

Protocols and Standards

- N/A

1.2 Applications

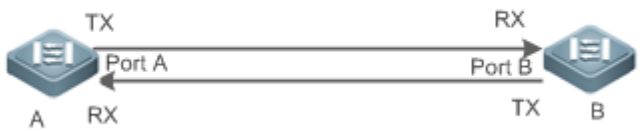
Application	Description
Configuring Unidirectional Link Detection	Detect unidirectional link failures.
Configuring Bidirectional Link Detection	Detect bidirectional link failures.
Configuring Downlink Loop Detection	Detect loop failures.

1.2.1 Configuring Unidirectional Link Detection

Scenario

As shown in Figure 1-1, device A is connected with device B through an optical fiber. The two lines are the Tx and Rx lines of the optical fiber. Unidirectional link detection of RLDP is enabled on device A and device B. If a fault occurs on either the Tx end of device A or Rx end of device B or on either the Rx end of device A or Tx end of device B, RLDP can detect the unidirectional failure and handle it. If the failure is eliminated, the administrator can manually restore the RLDP state on devices A and B and restart detection.

Figure 1-1



Remarks	A and B are layer-2 or layer-3 devices. The Tx end of port A on device A is connected with the Rx end of port B on device B. The Rx end of port A on device A is connected with the Tx end of port B on device B.

Deployment

- Enable RLDP globally.
- Configure unidirectional link detection of RLDP on ports and define a method for handling unidirectional failures.

1.2.2 Configuring Bidirectional Link Detection

Scenario

As shown in Figure 1-2, device A is connected with device B through an optical fiber. The two lines are the Tx and Rx lines of the optical fiber. Bidirectional link detection of RLDP is enabled on device A and device B. If a fault occurs on the Tx end of device A and Rx end of device B or on the Rx end of device A and Tx end of device B, RLDP can detect a bidirectional failure and handle it. If the failure is eliminated, the administrator can manually restore the RLDP state on devices A and B and restart detection.

Figure 1-2



Remarks	A and B are layer-2 or layer-3 devices. The Tx end of port A on device A is connected with the Rx end of port B on device B. The Rx end of port A on device A is connected with the Tx end of port B on device B.

Deployment

- Enable RLDP globally.
- Configure bidirectional link detection of RLDP on ports and define a method for handling bidirectional failures.

1.2.3 Configuring Downlink Loop Detection

Scenario

As shown in Figure 1-3, devices A, B, and C form a network loop. Downlink loop detection of RLDP is enabled on device A. RLDP can detect loop failures and make responses.

Figure 1-3



Remarks	A, B, and C are layer-2 or layer-3 devices. A, B, and C are interconnected through switching ports.

Deployment

- Enable global RLDP on device A.
- Configure downlink loop detection of RLDP for the ports that connect A and B and that connect A and C and define a method for handling loop failures.

1.3 Features

A typical Ethernet link detection mechanism detects physical link connectivity through auto-negotiation at the physical layer. However, this detection mechanism has limitations. In some cases, devices are connected and work normally at the physical layer but L2 link communication fails or is abnormal. RLDP recognizes a neighbor device and detects whether a link failure exists by exchanging prob packets, echo packets, or loop packets with the neighbor device.

Basic Concepts

Unidirectional Link Failure

A unidirectional link failure occurs when two optical fibers are crossly connected, one optical fiber is not connected or disconnected, one line in a twisted-pair cable is disconnected, or unidirectional disconnection occurs on an intermediate device between two devices. A unidirectional link failure can lead to incorrect forwarding of traffic or the failure of a loop protection protocol such as Spanning Tree Protocol (STP).

Bidirectional Link Failure

A bidirectional link failure occurs when two optical fibers are disconnected, two lines in a twisted-pair cable are disconnected, or bidirectional disconnection occurs on an intermediate device between two devices. A bidirectional link failure can lead to the incorrect forwarding of traffic.

Loop Failure

A loop failure occurs when a downlink port of a device is incorrectly connected with another device and a loop is formed. A loop failure can result in a broadcast storm.

RLDP Packet

RLDP packets include prob packets, echo packets, and loop packets.

- Prob packets: L2 multicast packets used for neighbor negotiation, and unidirectional or bidirectional link detection. The default packet encapsulation format is the Subnetwork Access Protocol (SNAP) type, which automatically changes to EthernetII if a neighbor sends EthernetII packets.
- Echo packets: L2 unicast packets in response to prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is of the SNAP type, which automatically changes to EthernetII if a neighbor sends EthernetII packets.
- Loop packets: L2 multicast packets for downlink loop detection. They can only be received by senders. The default encapsulation format of the packets is of the SNAP type.

RLDP Detection Interval and Maximum Detection Count

A detection interval and the maximum detection count can be configured for RLDP. A detection interval determines the period of sending prob packets and loop packets. When a device receives a prob packet, it replies with an echo packet immediately. A detection interval and the maximum detection count determine the maximum detection time (Detection interval × Maximum detection count + 1) for unidirectional or bidirectional link detection. If neither a prob nor an echo packet from a neighbor is correctly received within the maximum detection time, the handling of unidirectional or bidirectional failures is triggered.

RLDP Neighbor Negotiation

When configured with unidirectional or bidirectional link detection, a port can learn a peer device as its neighbor. One port can learn only one neighbor, which is changeable. If the negotiation function is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation. Negotiation is considered successful if the port receives a prob packet from the neighbor. However, if RLDP is enabled on a port after a failure occurs, the port fails to learn a neighbor and detection fails to be started. In this case, you are advised to rectify the link failure first.

Handling Methods for RLDP Failed Ports

- Warning: Only the relevant system log is printed to indicate the failed port and the failure type.
- Shutdown SVI: A system log is printed. If the failed port is a physical switching port or member port of an L2 aggregate port (AP), the switch virtual interface (SVI) is queried based on the access virtual local area network (VLAN) or native VLAN of the port, and then the SVI is shut down.
- Errdisable: A system log is printed, the failed port is set to the errdisable state, and the port enters the linkdown state physically.
- isolate-vlan: A system log is printed, and the looped VLAN is isolated.

Recovery Methods for RLDP Failed Ports

- Manual reset: Manually reset all the failed ports to the initialized state to restart link detection.
- Manual or automatic execution of **errdisable recovery**: Recover all the failed ports to the initialized state manually or regularly (30s by default and configurable) and restart link detection.
- Automatic recovery: Under unidirectional or bidirectional link detection, if the handling method specified for failed ports is not entering the errdisable state, the ports can automatically recover to the initialized state based on prob packets exchanged with the neighbor and restart link detection.
- Automatic execution of **rldp error-recover interval**: Recover all the failed ports to the initialized state regularly (configurable) and restart link detection.

RLDP Port Status

- normal: Indicates the state of a port, on which link detection is enabled.
- error: Indicates the state of a port, on which a unidirectional or bidirectional link failure or a loop failure is detected.

Overview

Feature	Description
Enabling RLDP Detection	Enable unidirectional link detection, bidirectional link detection, or downlink loop detection to discover unidirectional, bidirectional, or loop failures and handle the failures.

1.3.1 Enabling RLDP Detection

RLDP provides unidirectional link detection, bidirectional link detection, downlink loop detection, and VLAN loop detection.

Working Principle

Unidirectional Link Detection

After unidirectional link detection is enabled, a port sends prob packets to and receives echo packets from a neighbor regularly. It also receives prob packets from the neighbor and replies with echo packets to the neighbor. If the port receives only prob packets but no echo packets, or none of them from the neighbor within the maximum detection time, handling of a unidirectional failure is triggered and the detection stops.

Bidirectional Link Detection

After bidirectional link detection is enabled, a port sends prob packets to and receives echo packets from a neighbor regularly. It also receives prob packets from the neighbor and replies with echo packets to the neighbor. If the port receives neither prob packets nor echo packets from the neighbor within the maximum detection time, handling of a bidirectional failure is triggered and the detection stops.

Downlink Loop Detection

After downlink loop detection is enabled on ports, the ports send loop packets regularly. A loop failure is triggered in the following scenarios: The transmission and receiving ports of the packets are the same routed port or L3 AP member port; the transmission and receiving ports of the packets are switching ports

or L2 AP member ports, the default VLANs of the ports are the same, and forwarding states of the ports are Forward. The failure is handled according to the configured method, and the detection stops.

Related Configuration

- Configure RLDP detection.

The detection function is disabled by default.

Run the **rldp enable** command in global configuration mode or the **rldp port** command in interface configuration mode to enable RLDP detection and specify the detection type and failure handling method.

Based on the actual environment, run the **rldp neighbor-negotiation** command to specify neighbor negotiation, the **rldp detect-interval** command to specify the detection interval, the **rldp detect-max** command to specify the maximum detection count, the **rldp error-recover interval** command to recover failed ports regularly, and the **rldp reset** command to recover failed ports.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic RLDP Functions	⚠ (Mandatory in global configuration mode) It is used to enable RLDP detection globally.	
	rldp enable	Enables RLDP detection globally to apply RLDP detection to all ports.
	⚠ (Mandatory in interface configuration mode) It is used to specify the detection type and failure handling method on a port.	
	rldp port	Enables RLDP detection on a port and specifies the detection type and failure handling method.
	⚠ (Optional in global configuration mode) It is used to specify the detection interval, maximum detection count, and whether neighbor negotiation is required.	
	rldp detect-interval **rldp detect-max** **rldp neighbor-negotiation**	Modifies RLDP configuration parameters globally, including the detection interval, maximum detection count, neighbor negotiation, which can take effect to RLDP detection on all ports.
	rldp error-recover interval	Configures an interval globally for RLDP to recover failed ports. No interval is configured by default.
	⚠ (Optional in privilege EXEC mode)	

	rldp reset	Recovers failed ports in privilege EXEC mode, which can take effect to RLDP detection on all ports.

1.4.1 Configuring Basic RLDP Functions

Configuration Effect

- Enable RLDP unidirectional link detection, bidirectional link detection, downlink loop detection, or VLAN loop detection to discover unidirectional, bidirectional, downlink loop, or VLAN loop failures.

Notes

- Loop detection configured on an AP member port takes effect on all the member ports of the AP. Unidirectional link detection and bidirectional link detection configured on an AP member port take effect only on the AP member port.
- The loop detection configuration of a physical port added to an AP must be the same as that of the other member ports of the AP. If loop detection is not configured on the new member port but on the existing member ports or loop detection configured on the new member port is different from that on existing member ports, the new port adopts the configuration and detection results of the existing member ports.
- When RLDP is configured on an AP member port, only the "shutdown-port" handling method can be configured. If the failure handling method is not "shutdown-port", it is modified to "shutdown-port" and takes effect.
- After the "shutdown-port" handling method is configured on a port, the port cannot resume RLDP detection in the case of a failure. After confirming that the failure is rectified, you can run the **rldp reset** or **errdisable recovery** command to restore the port and restart detection.

Configuration Steps

↘ Enabling RLDP Detection Globally

- Mandatory.
- After RLDP detection is configured in global configuration mode, RLDP detection can be started on all ports.

↘ Configuring Neighbor Negotiation Globally

- Optional.
- After neighbor negotiation is configured in global configuration mode, RLDP detection on a port is started after successful neighbor negotiation.

↘ Configuring the Detection Interval Globally

- Optional.
- Configure the detection interval in global configuration mode.

Configuring the Maximum Detection Count Globally

- Optional.
- In global configuration mode,
- specify the maximum detection count.

Configuring the Interval for Recovering Failed Ports Globally

- Optional.
- Configure the interval for recovering failed ports in global configuration mode.

Enabling RLDP Detection on a Port

- Mandatory.
- Perform this configuration in interface configuration mode.
- In interface configuration mode, configure unidirectional link detection, bidirectional link detection, downlink loop detection, or VLAN loop detection of RLDP and specify a failure handling method.

Recovering All Failed Ports in Privileged EXEC Mode

- Optional.
- Perform this configuration in privileged EXEC mode to restore all the failed ports and restart detection.

Verification

- Display RLDP information on the device, including global, port, and neighbor information.

Related Commands

Enabling RLDP Globally

Command	rldp enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to enable RLDP detection globally.

Enabling RLDP Detection on a Port

Command	**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port }**
Parameter Description	**unidirection-detect**: Enables unidirectional link detection. **bidirection-detect**: Enables bidirectional link detection. **loop-detect**: Enables downlink loop detection. **warning**: Sends a warning upon a failure. **shutdown-svi**: Disables the SVI to which a port belongs upon a failure. **shutdown-port**: Sets a port to the errdisable state upon a failure.
Command Mode	Interface configuration mode
Usage Guide	Ports include layer-2 switching ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports. The port that detects a downlink loop failure is at random. For example, if RLDP downlink loop detection is configured on downlink ports A and B, the configured failure handling method is warning on downlink port A and shutdown-port on downlink port B, and a downlink loop exists between ports A and B, port A may detect a downlink loop failure before port B. After the failure handling method on port A takes effect, port A no longer sends packets or detects the downlink loop status. Port B does not receive prob packets from port A and cannot detect downlink loop failures. As a result, the downlink loop failure still exists in the environment. To ensure that downlink loop failures in actual scenarios can be rectified, the loop failure handling method configured on downlink ports in the same loop must be the same and cannot be warning. The monitor policy can be configured in unidirectional link detection mode for association with the Ethernet Ring Protection Switching (ERPS) protocol to ensure that ERPS can detect unidirectional link connection in time.

Modifying RLDP Detection Parameters Globally

Command	**rldp** { **detect-interval** *interval* | **detect-max** *num* | **neighbor-negotiation** }
Parameter Description	**detect-interval** *interval*: Specifies the detection interval. **detect-max** *num*: Specifies the maximum detection count. **neighbor-negotiation**: Specifies whether neighbor negotiation is required.
Command Mode	Global configuration mode
Usage Guide	This command is used to modify all RLDP detection parameters for all ports when the actual environment changes.

Configuring the Interval for Recovering Failed Ports Globally

Command	**rldp error-recover interval** *interval*
Parameter Description	*interval*: Interval for recovering failed ports, in seconds. The value range is from 30 to 86400. By default, no interval is configured.
Command Mode	Global configuration mode
Usage Guide	This command is used to recover RLDP failed ports regularly. If a loop failure is rectified, the environment can be restored automatically.

Recovering RLDP Failed Ports

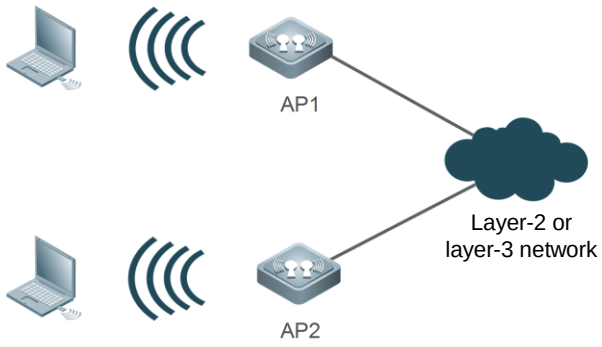
Command	**rldp reset**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to reset all RLDP failed ports and restart detection.

Displaying RLDP Status Information

Command	**show rldp** [**interface** *interface-type interface-number*]
Parameter Description	*interface-type interface-number*: Name of the interface to be queried.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	This command is used to display the status information of RLDP.

Configuration Example

Configuring RLDP Loop Detection on Wireless APs

Scenario **Figure 1-4**	As shown in Figure 1-5, RLDP loop detection is configured on wireless APs. 
Configuration Steps	● Enable RLDP loop detection on the AP wired ports. ● Enable RLDP on APs in global configuration mode. ● On APs, configure the recovery time for ports that are set to the errdisable state by RLDP.
AP1, AP2	Hostname#configure terminal Hostname(config)# rldp enable Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# errdisable recovery interval 500 Hostname(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
Verification	● On the AP, check whether the RLDP loop detection configurations take effect.
AP1, AP2	Hostname# show run ! rldp enable ...

	interface GigabitEthernet 0/1 errdisable recovery interval 500 encapsulation dot1Q 1 rldp port loop-detect shutdown-port !

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays the RLDP running status.	**show rldp** [**interface** *interface-type interface-number*]

Configuring Network Management and Monitoring

1. Configuring NTP
2. Configuring SNTP
3. Configuring FTP Server
4. Configuring FTP Client
5. Configuring TFTP Client
6. Configuring SNMP
7. Configuring RMON
8. Configuring CWMP
9. Configuring RPCAP

1 Configuring NTP

1.1 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, the 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)

1.2 Applications

Application	Description
Synchronizing Time Based on an External Reference Clock Source	A device is used as a client that synchronizes time with an external clock source. After successful synchronization, it is used as a server to provide time synchronization for other devices.
Synchronizing Time Based on a Local Reference Clock Source	A device uses a local clock as a reliable NTP reference clock source and is also used as a server to provide time synchronization for other devices.

1.2.1 Synchronizing Time Based on an External Reference Clock Source

Scenario

As shown in Figure 1-1:

- 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 1-1



Deployment

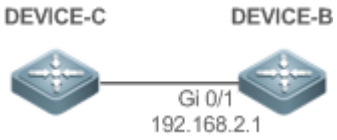
Configure DEVICE-B to the NTP external reference clock mode.

1.2.2 Synchronizing Time Based on a Local Reference Clock Source

Scenario

As shown in Figure 1-2, DEVICE-B uses a local clock as the NTP reference clock source and provides time synchronization for DEVICE-C.

Figure 1-2



Deployment

Configure DEVICE-B to the NTP local reference clock mode.

1.3 Features

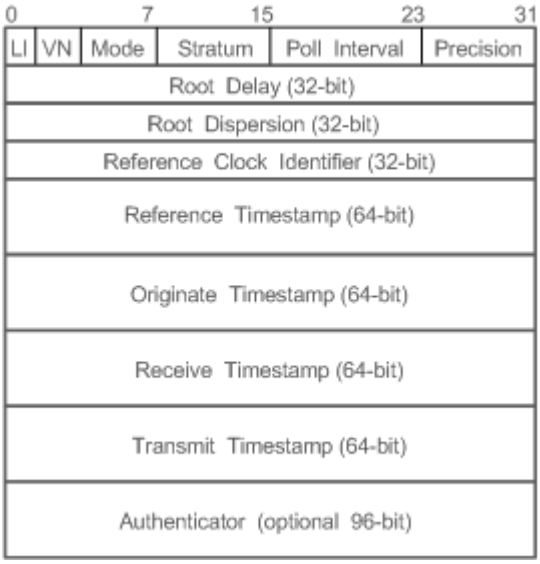
Basic Concepts

NTP Packet

As defined in RFC1305, NTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 1-3 shows the format of an NTP time synchronization packet.

Figure 1-3 Format of an NTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP version number. The current version number is 3.
- Mode: indicates a 3-bit NTP working mode.

0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master reference clock source; other values: indicate slave reference clock sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master reference clock source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

NTP Server

A device uses a local clock as the reference clock source to provide time synchronization for other devices in the network.

NTP Client

A device is used as an NTP client that synchronizes time with an NTP server in the network.

Stratum

In NTP, "stratum" is used to describe the hops from a device to an authority clock source. An NTP server whose stratum is 1 has a directly connected atomic clock or radio controlled clock; an NTP server whose stratum is 2 obtains time from the server whose stratum is 1; an NTP server whose stratum is 3 obtains time from the server whose stratum is 2; and so on. Therefore, clock sources with lower stratums have higher clock precisions.

Hardware Clock

A hardware clock operates based on the frequency of the quartz crystal resonator on a device and is powered by the device battery. After the device is shut down, the hardware clock continues running. After the device is started, the device obtains time information from the hardware clock as the software time of the device.

Overview

Feature	Description
NTP Time Synchronization	Network devices synchronize time with their servers or reliable clock sources to implement high-precision time correction.
NTP Security Authentication	The NTP packet encryption authentication is used to prevent unreliable clock sources from time synchronization interference on a device.
NTP Access Control	An Access Control List (ACL) is used to filter sources of received NTP packets.

1.3.1 NTP Time Synchronization

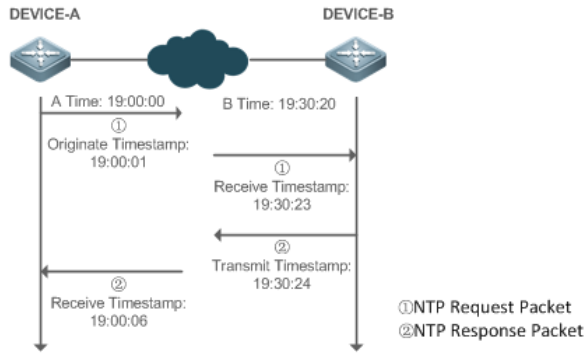
Working Principle

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 1-4 shows the format of an NTP time synchronization packet.

Figure 1-4 Working Principle of NTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an NTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

1. A sends an NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
2. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
3. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
4. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.

- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

NTP Working Mode

- External clock reference mode

In this mode, a device is used as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server first and provide time synchronization for the clients after successful synchronization.

- Local clock reference mode

In this mode, a device uses the default local clock as the reliable clock source and provides time synchronization directly for other clients.

Related Configuration

Configuring an NTP Server

- The NTP function is disabled by default.
- Run the **ntp server** command to specify an NTP server (external clock reference source), which can enable NTP.
- After the configuration, the device works in the external clock reference mode.

Real-time Synchronization

- A device performs time synchronization every 64 seconds by default.

Updating a Hardware Clock

- By default, a device does not update synchronized time to the hardware clock.
- Run the **ntp update-calendar** command to enable a device to automatically update the hardware clock after successfully synchronizing time each time.

Configuring the NTP Master Clock

- By default, a device works in the external clock reference mode.
- Run the **ntp master** command to configure a device to the local clock reference mode.

1.3.2 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.

1.3.3 NTP Access Control

Working Principle

Provide a minimum security measure by using an ACL.

Related Configuration

Configuring the Access Control Rights for NTP Services

- By default, there is no access control right for NTP.
- Run the **ntp access-group** command to configure the access control rights for NTP.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of NTP	⚠ (Mandatory) It is used to enable NTP. After NTP is enabled, a device works in the external clock reference mode.	
	ntp server	Configures an NTP server.
	ntp update-calendar	Automatically updates a hardware clock.
	⚠ (Optional) It is used to configure a device to the local clock reference mode.	
	ntp master	Configures the NTP master clock.
	⚠ (Optional) It is used to configure the local clock reference mode for devices.	

	ntp interval	Configures the interval for time synchronization between the NTP client and the NTP server.
	(Optional) It is used to disable NTP.	
	no ntp	Disables all functions of NTP and clears all NTP configurations.
	ntp disable	Disables receiving of NTP packets from a specified interface.
	ntp service disable	Disables the NTP time synchronization service.
Configuring NTP Security Authentication	(Optional) It is used to prevent unreliable clock sources from performing time synchronization interference on a device.	
	ntp authenticate	Enables a security authentication mechanism.
	ntp authentication-key	Configures a global authentication key.
	ntp trusted-key	Configures a trusted key for time synchronization.
	ntp server	Configures a trusted key for an external reference clock source.
Configuring NTP Access Control	(Optional) It is used to filter the sources of received NTP packets.	
	ntp access-group	Configures the access control rights for NTP.

1.4.1 Configuring Basic Functions of NTP

Configuration Effect

External Clock Reference Mode

- Use a device as a client to synchronize time from an external reference clock source to the local clock.
- After the time synchronization is successful, use the device as a time synchronization server to provide time synchronization.

Local Clock Reference Mode

- Use the local clock of a device as the NTP reference clock source to provide time synchronization.

Notes

- In the client/server mode, a device can be used as a time synchronization server to provide time synchronization only after successfully synchronizing time with a reliable external clock source.
- Once the local clock reference mode is configured, the system will not synchronize time with a clock source with a higher stratum.

- Configuring a local clock as the master clock (especially when specifying a lower stratum) may overwrite an effective clock source. If this command is used for multiple devices in a network, the clock difference between the devices may cause unstable time synchronization of the network.
- Before a local clock is configured as the master clock, if the system never synchronizes time with an external clock source, you may need to manually calibrate the system clock to ensure that there is no excessive difference. For details about how to manually calibrate the system clock, refer to the system time configuration section in the configuration guide.

Configuration Steps

Configuring an NTP Server

- (Mandatory) At least one external reference clock source must be specified (A maximum of 20 different external reference clock sources can be configured).
- If it is necessary to configure an NTP key, you must configure NTP security authentication before configuring the NTP server.

Configuring the Interval for Time Synchronization with the External Server

- To customize the interval for time synchronization, run this command.
- The default NTP time synchronization interval is 64s.

Automatically Updating a Hardware Clock

- Optional.
- By default, the system updates only the system clock, but not the hardware clock after successful time synchronization.
- After this command is configured, the system automatically updates the hardware clock after successful time synchronization.

Configuring the NTP Master Clock

- To switch a device to the local clock reference mode, run this command.

Configuring the Interval for Time Synchronization Between the NTP Client and the NTP Server

- The default NTP time synchronization interval is 64s.

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.

Disabling the NTP Device to Provide Time Synchronization Service for Other Devices

- If an NTP device works in client/server mode, after the NTP device synchronizes time from an external reliable clock source, the device acts as the time server to provide the time synchronization service for other devices. If you want the NTP device to act simply as a client, configure the **ntp service disable** command to disable the NTP device to provide time synchronization service for other devices.

Verification

- Run the **show ntp status** command to display the NTP configuration.
- Run the **show clock** command to check whether time synchronization is completed.

Related Commands

Configuring an NTP Server

Command	**ntp server** { *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *interface*] [**key** *keyid*] [**prefer**]
Parameter Description	*ip-addr*: Indicates the IPv4/IPv6 address of the reference clock source. *domain*: Indicates the IPv4/IPv6 domain name of the reference clock source. *version*: Indicates the NTP version number, ranging from 1 to 3. *interface*: Indicates the interface type, including AggregatePort, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and Vlan. *keyid*: Indicates the key used for encrypted communication with the corresponding server. It is not encrypted by default. The value ranges from 1 to 4,294,967,295. **prefer**: Indicates whether the reference clock source has a high priority.
	Specifies the egress management interface for packets in the oob mode.
Command Mode	Global configuration mode
Usage Guide	By default, no NTP server is configured. Client system supports interaction with up to 20 NTP servers. You can configure an authentication key for each server (after configuring global authentication and the related key) to initiate encrypted communication with the servers. ⚠ If it is necessary to configure an authentication key, you must configure NTP security authentication before configuring an NTP server. The default version of NTP for communicating with a server is NTP version 3. In addition, you can configure the source interface for transmitting NTP packets and specify that the NTP packets from a corresponding server can be received only on the transmitting interface.

Configuring the Interval for Time Synchronization Between the NTP Client and the NTP Server

Command	**ntp interval** *seconds*
Parameter Description	*seconds*: Indicates the interval for time synchronization in seconds. The value ranges from 10 to 2,592,000. The default value is 64.
Command Mode	Global configuration mode
Usage Guide	N/A

Updating a Hardware Clock

Command	**ntp update-calendar**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Configuring a Local Reference Clock Source

Command	**ntp master**[*stratum*]
Parameter Description	*stratum*: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling NTP

Command	**no ntp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command can be used to fast disable all functions of NTP and clear all NTP configurations.

Disabling Receiving of NTP Packets on an Interface

Command	**ntp disable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Disabling the NTP Device to Provide Time Synchronization for Other Devices

Command	**ntp server disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command disables the NTP time synchronization service. After this command is configured, external devices cannot be synchronized time from the NTP device (this command is supported only in some versions).

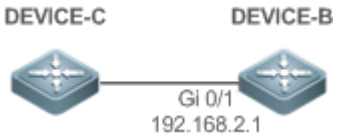
Configuration Example

External Clock Reference Mode of NTP

Scenario **Figure 1-5**	
	● DEVICE-B is configured to the NTP external clock reference mode.

	● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-A configures the local clock as the NTP reference clock source. ● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-A	A#configure terminal A(config)# ntp master A(config)#exit
DEVICE-B	B#configure terminal B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show ntp status** command on DEVICE-B to display the NTP configuration. ● DEVICE-B sends a time synchronization packet to 192.168.1.1 in order to synchronize time with DEVICE-A. ● After successfully synchronizing time with DEVICE-A, DEVICE-B can respond to the time synchronization request from DEVICE-C. ● Run the **show clock** command on DEVICE-B and DEVICE-C to check whether the time synchronization is successful.

↘ Local Clock Reference Mode of NTP

Scenario Figure 1-6	
	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp master B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1

	C(config)# exit
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful.

1.4.2 Configuring NTP Security Authentication

Configuration Effect

Synchronizing Time from a Trusted Reference Clock Source

Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock.

Providing Time Synchronization for a Trusted Device

Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

Notes

The authentication keys of the client and server must be the same.

Configuration Steps

Configuring a Global Security Authentication Mechanism for NTP

- Mandatory.
- By default, a device disables the security authentication mechanism.

Configuring a Global Authentication Key for NTP

- Mandatory.
- By default, a device is not configured with an authentication key.

Configuring a Globally Trusted Key ID for NTP

- Optional.
- To provide time synchronization for a trusted device, you must specify a trusted authentication key by using the key ID.
- Only one trusted key can be configured. The specified authentication key must be consistent with that of the trusted device.

Configuring an Authentication Key ID for an External Reference Clock Source

- Optional.
- To synchronize time with a trusted reference clock source, you must specify a trusted authentication key by using the key ID.
- Each trusted reference clock source is mapped to an authentication key. The authentication keys must be consistent with the keys of trusted reference clock sources.

Verification

- Run the **show run** command to verify the NTP configuration.
- Run the **show clock** command to check whether time is synchronized only with a trusted device.

Related Commands

Enabling a Security Authentication Mechanism

Command	**ntp authenticate**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, a client does not use a global security authentication mechanism. If no security authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that the communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must also be configured for initiating encrypted communication between the client and server.

Configuring a Global Authentication Key

Command	**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]
Parameter Description	*key-id*: indicates the ID of a global authentication key, ranging from 1 to 4294967295. *key-string*: Indicates a key string. A non-encrypted key string contains up to 31 bytes. An encrypted key string contains up to 64 bytes. *enc-type*: (optional) indicates whether an entered key is encrypted. 0 indicates no encryption, and 7 indicates simple encryption. The default setting is no encryption.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for NTP

Command	**ntp trusted-key** *key-id*
Parameter Description	*key-id*: Indicates the ID of a trusted key, ranging from 1 to 4294967295.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for an External Reference Clock Source

Refer to the section "Related Commands

Configuration Example

Security Authentication

Scenario **Figure 1-7**	
	● DEVICE-B is configured to the NTP client/server mode and provides NTP services requiring security authentication for DEVICE-C. The authentication key is "abcd". ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp authenticate B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authenticate C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp trusted-key 1 C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
Verification	● DEVICE-B sends a time synchronization packet that carries authentication information to 192.168.1.1 in order to synchronize time with DEVICE-A. ● Run the **show clock** command on DEVICE-B to check whether the time synchronization is successful.

1.4.3 Configuring NTP Access Control

Configuration Effect

Access control for NTP services provides a minimum security measure. A more secure method is to use an NTP authentication mechanism.

Notes

- Currently, the system does not support control query (used to control NTP servers by using network management devices, such as setting the leap second indicator or monitoring its working status). Though rule matching is implemented in the preceding sequence, no request related to control query is supported.

- If no access control rule is configured, all accesses are allowed. If any access control rule is configured, only accesses allowed by the rule can be implemented.

Related Configuration

Configuring the Access Control Rights for NTP

- Optional.
- Run the **ntp access-group** command to configure the access control rights and a corresponding ACL for NTP.

Verification

Run the **show run** command to verify the NTP configuration.

Related Commands

Configuring the Access Control Rights for NTP Services

Command	**ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*
Parameter Description	**peer**: allows time request and control query for local NTP services, and allows a local device to synchronize time with a remote system (full access rights). **serve**: allows time request and control query for local NTP services, but does not allow a local device to synchronize time with a remote system. **serve-only**: allows only time request for local NTP services. **query-only**: allows only control query for local NTP services. *access-list-number*: indicates the number of an IP ACL, ranging from 1 to 99 and from 1300 to 1999. For details about how to create an IP ACL, refer to the *Configuring ACL*. *access-list-name*: indicates the name of an IP ACL. For details about how to create an IP ACL, refer to the *Configuring ACL*.
Command Mode	Global configuration mode
Usage Guide	Configure NTP access control rights. When an access request arrives, the NTP service matches rules in the sequence from the minimum access restriction to the maximum access restriction and uses the first matched rule. The matching sequence is peer, serve, serve-only, and query-only.

Configuration Example

Configuring NTP Access Control Rights

Configuration Steps	Allow only the device with the IP address of 192.168.1.1 to send a time synchronization request to a local device.
	Hostname(config)# access-list 1 permit 192.168.1.1 Hostname(config)# ntp access-group serve-only 1

1.5 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**

1 Configuring SNTP

1.1 Overview

The Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (NTP), which is used to synchronize the clocks of computers on the Internet. SNTP is applied in scenarios where it is unnecessary to use all NTP functions.

NTP uses a complex algorithm and has higher requirements for the system whereas SNTP uses a simpler algorithm and provides higher performance. Generally, SNTP precision can reach about 1s, which meets the basic requirements of most scenarios. Since SNTP packets are the same as NTP packets, the SNTP client implemented on a device is fully compatible with an NTP server.

Protocols and Standards

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

1.2 Applications

Application	Description
Synchronizing Time with an NTP Server	A device is used as a client to synchronize time with an NTP server.

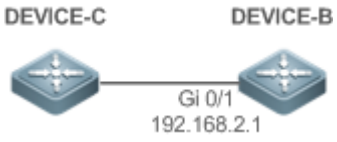
1.2.1 Synchronizing Time with an NTP Server

Scenario

As shown in Figure 1-1, DEVICE-B uses a local clock as the NTP clock reference source and provides time synchronization for DEVICE-C.

DEVICE-C is used as an SNTP client to synchronize time with DEVICE-B.

Figure 1-1



Deployment

- Specify DEVICE-B as the SNTP server of DEVICE-C.
- Enable SNTP for DEVICE-C.

1.3 Features

Basic Concepts

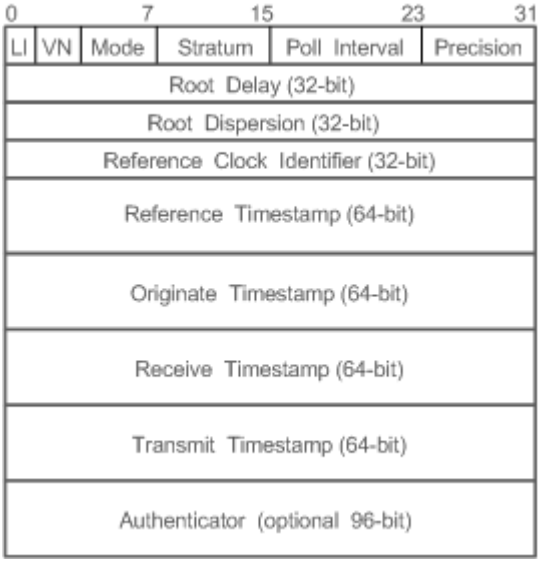
SNTP Packet

SNTPV4 is developed from NTP, which is intended to simplify the functions of NTP. It does not change the NTP specifications and the original implementation of NTP. The message format of SNTPV4 is the same as that of NTP defined in RFC1305, with only some data fields initialized into preset values.

As defined in RFC1305, SNTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 1-2 shows the format of an SNTP time synchronization packet.

Figure 1-2 Format of an SNTP 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/SNTP version number. The current version number is 3.
- Mode: indicates a 3-bit SNTP/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 clock reference source; other values: indicate slave clock reference 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 clock reference 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.

Overview

Feature	Description
SNTP Time Synchronization	Synchronizes time from an SNTP/NTP server to a local device.

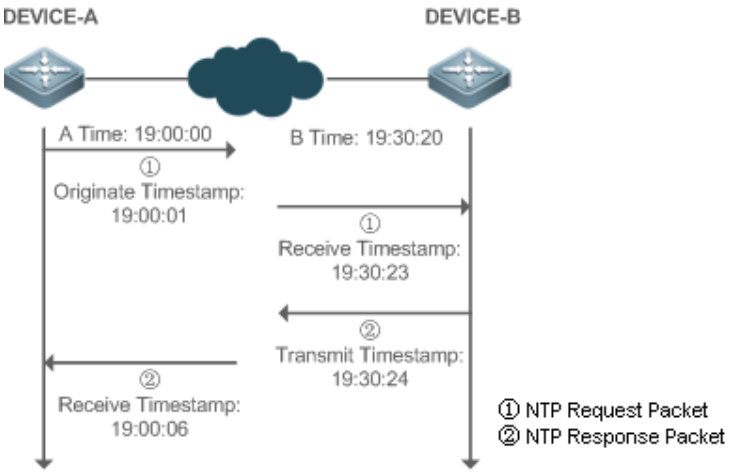
1.3.1 SNTP Time Synchronization

Working Principle

SNTP time synchronization is implemented by interaction of SNTP/NTP packets between a client and a server. The client sends a time synchronization packet to the server at intervals (half an hour by default). After receiving a response packet from the server, the client synchronizes time.

Figure 1-3 shows the format of an SNTP time synchronization packet.

Figure 1-3 Working Principle of SNTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an SNTP 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 SNTP/NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
2. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.

3. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
4. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

Related Configuration

Enabling SNTP

- SNTP is disabled by default.
- Run the **sntp enable** command to enable SNTP.

Configuring an SNTP Server

- By default, no SNTP server is configured.
- Run the s**ntp server** command to specify an SNTP server.

Configuring the SNTP Time Synchronization Interval

- By default, the SNTP time synchronization interval is 1,800s.
- Run the **sntp interval** command to specify the SNTP time synchronization interval.

1.4 Configuration

Configuration	Description and Command	
Configuring SNTP	(Mandatory) It is used to enable SNTP.	
	sntp enable	Enables SNTP.
	sntp server	Configures the IP address of an SNTP server.
	(Optional) It is used to configure the SNTP time synchronization interval.	
	sntp interval	Configures the SNTP time synchronization interval.

1.4.1 Configuring SNTP

Configuration Effect

An SNTP client accesses an NTP server at fixed intervals to correct the clock regularly.

Notes

All time obtained through SNTP communication is Greenwich Mean Time (GMT). To obtain precise local time, you need to set the local time zone for alignment with GMT.

Configuration Steps

Enabling SNTP

- (Mandatory) SNTP is disabled by default.

Configuring the IP address of an SNTP Server

- (Mandatory) No SNTP/NTP server is configured by default.

Configuring the SNTP Time Synchronization Interval

- Optional.
- By default, a device synchronizes time every half an hour.

Verification

Run the **show sntp** command to display SNTP-related parameters.

Related Commands

Enabling SNTP

Command	**sntp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	SNTP is disabled by default. Run the **no sntp enable** global configuration command to disable SNTP.

Configuring the IP address of an SNTP Server

Command	**sntp server** { *ip-address* | *domain* } [**source** *source-ip-address*]
Parameter Description	*ip-address*: Indicates the IP address of an SNTP server. No SNTP server is configured by default. *domain:* Indicates the domain name of an SNTP server. No SNTP server is configured by default. *source-ip-address*: Indicates the source IP address of an SNTP server.
Command Mode	Global configuration mode
Usage Guide	Since SNTP is fully compatible with NTP, the server can be configured as a public NTP server on the Internet. Since SNTP packets are the same as NTP packets, the SNTP client is fully compatible with the NTP server. There are many NTP servers on the Internet. You can select an NTP server with a shorter delay as the SNTP server on your device.

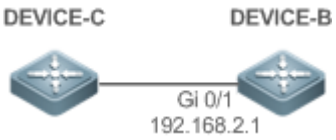
Configuring the SNTP Time Synchronization Interval

Command	**sntp interval** *seconds*

Parameter Description	*seconds*: Indicates the interval for time synchronization in seconds. The value ranges from 60 to 65,535. The default value is 1,800s.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the interval for an SNTP client to synchronize time with an NTP/SNTP server. ⚠ The interval configured here does not take effect immediately. To make it take effect immediately, run the **sntp enable** command.

Configuration Example

SNTP Time Synchronization

Scenario Figure 1-4	
	● DEVICE-B indicates an NTP server on the Internet. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	Enable SNTP for DEVICE-C and configure DEVICE-B as an NTP server.
DEVICE-C	C#configure terminal C(config)# sntp server 192.168.2.1 C(config)# sntp enable C(config)# exit
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful. ● Run the **show sntp** command on DEVICE-C to display the SNTP status and check whether the server is successfully configured.

1.5 Monitoring

Displaying

Description	Command
Displays SNTP-related parameters.	**show sntp**

Debugging

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

Description	Command
Enables debugging.	**debug sntp**

1 Configuring FTP Server

1.1 Overview

The File Transfer Protocol (FTP) server function enables a device to serve as an FTP server. In this way, a user can connect an FTP client to the FTP server and upload files to and download files from the FTP server through FTP.

A user can use the FTP server function to easily obtain files such as syslog files from a device and copy files to the file system of the device through FTP.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)
- RFC3659: Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC2428: FTP Extensions for IPv6 and NATs
- RFC1635: How to Use Anonymous FTP

1.2 Applications

Application	Description
Providing FTP Services in a LAN	Provides the uploading and downloading services for a user in a Local Area Network (LAN).

1.2.1 Providing FTP Services in a LAN

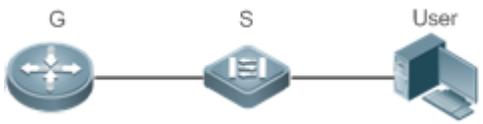
Scenario

Provide the uploading and downloading services for a user in a LAN.

As shown in Figure 1-1, enable the FTP server function only in a LAN.

- G and S are enabled with the FTP server function and layer-2 transparent transmission function respectively.
- A user initiates a request for FTP uploading and downloading services.

Figure 1-1



Remarks	G is an egress gateway device. S is an access device.

Deployment

- G is enabled with the FTP server function.
- As a layer-2 switch, S provides the function of layer-2 transparent transmission.

1.3 Features

Basic Concepts

FTP

FTP is a standard protocol defined by the IETF Network Working Group. It implements file transfer based on the Transmission Control Protocol (TCP). FTP enables a user to transfer files between two networked computers and is the most important approach to transferring files on the Internet. A user can obtain abundant Internet for free through anonymous FTP. In addition, FTP provides functions such as login, directory query, file operation, and other session control. Among the TCP/IP protocol family, FTP is an application-layer protocol and uses TCP ports 20 and 21 for transmission. Port 20 is used to transmit data and port 21 is used to transmit control messages. Basic operations of FTP are described in RFC959.

User Authorization

To connect an FTP client to an FTP server, you should have an account authorized by the FTP server. That is, a user can enjoy services provided by the FTP server after logging in to the FTP server with a user name and password. A maximum of 10 accounts can be configured, a maximum of 2 connections are allowed for each account, and a maximum of 10 connections are supported by the server.

FTP File Transmission Modes

FTP provides two file transmission modes:

- Text transmission mode (ASCII mode): It is used to transfer text files (such as .txt, .bat, and .cfg files). This mode is different from the binary mode in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to local CRC characters, for example, \n in Unix, \r\n in Windows, and \r in Mac. Assume that a file being copied contains ASCII text. If a remote computer does not run Unix, FTP automatically converts the file format to suit the remote computer.
- Binary transmission mode: It is used to transfer program files (for example, .app, .bin and .btm files), including executable files, compressed files and image files without processing data. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

FTP Working Modes

FTP provides two working modes:

Figure 1-2

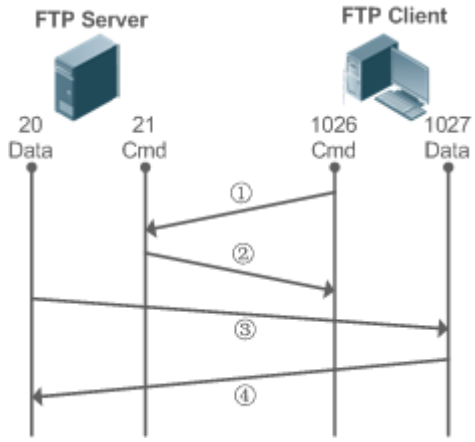
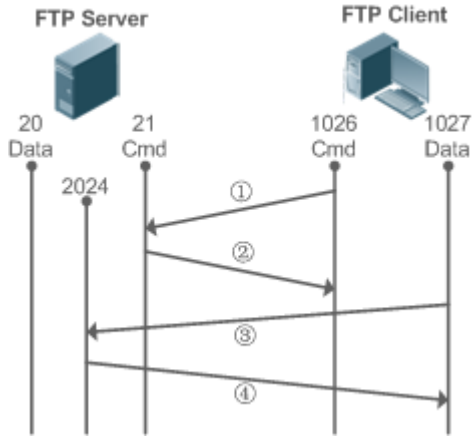


Figure 1-3



- Figure 1-2 shows the active (PORT) mode. The FTP client uses port 1026 to connect to the FTP server through port 21. The client sends commands through this channel. Before receiving data, the client sends the **PORT** command on this channel. The **PORT** command contains information on the channel port (1027) of the client for receiving data. The server uses port 20 to connect to the client through port 1027 for establishing a data channel to receive and transmit data. The FTP server must establish a new connection with the client for data transmission.
- Figure 1-3 shows the passive (PASV) mode. The process for establishing a control channel is similar to that in the PORT mode. However, after the connection is established, the client sends the **PASV** command rather than the **PORT** command. After receiving the **PASV** command, the FTP server enables a high-end port (2024) at random and notifies the client that data will be transmitted on this port. The client uses port 1027 to connect the FTP server through port 2024. Then, the client and server can transmit and receive data on this channel. In this case, the FTP server does not need to establish a new connection with the client.

↘ Supported FTP Commands

After receiving an FTP connection request, the FTP server requires the client to provide the user name and password for authentication.

If the client passes the authentication, the FTP client commands can be executed for operations. The available FTP client commands are listed as follows:

ascii	delete	mdelete	mput	quit	send

bin	dir	mdir	nlist	recv	size
bye		mget		rename	system
cd	get	mkdir	passive		type
cdup		mls	put	rmdir	user
close	ls		pwd		

For usage of these FTP client commands, please refer to your FTP client software document. In addition, many FTP client tools (such as CuteFTP and FlashFXP) provide the graphic user interface. These tools facilitate operations by freeing users from configuring FTP commands.

Overview

Feature	Description
Enabling the FTP Server Function	Provides the functions of uploading, downloading, displaying, creating and deleting files for an FTP client.

1.3.1 Enabling the FTP Server Function

Working Principle

The basic working principle is described in the previous chapter. Ruijie devices provide FTP services after the user name, password, and top-level directory are configured.

Related Configuration

Enabling the FTP Server Function Globally

The FTP server function is disabled by default.

Run the **ftp-server enable** command to enable the FTP server function.

You must enable the FTP server function globally before using it.

Configuring a User Name, Password, and Top-Level Directory

There is no authorized user or top-level directory by default.

Run the **ftp-server usernamepassword** and **ftp-server topdir** commands to set an authorized user and top-level directory.

The three configurations above are mandatory; otherwise, the FTP server function cannot be enabled.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	⚠ (Mandatory) It is used to enable an FTP server.	
	ftp-server enable	Enables the FTP server function.

	ftp-server login timeout	Configures Login timeout for an FTP session.
	ftp-server login times	Configures the valid login count.
	ftp-server topdir	Configures the top-level directory of the FTP server.
	ftp-server username password	Configures a user name and password.
	⚠ Optional.	
	ftp-server timeout	Configures the idle timeout of an FTP session.

1.4.1 Configuring Basic Functions

Configuration Effect

- Create an FTP server to provide FTP services for an FTP client.

Notes

- The user name, password, and top-level directory need to be configured.
- To enable the server to close an abnormal session within a limited period, you need to configure the idle timeout of a session.

Configuration Steps

↘ Enabling the FTP Server Function

- Mandatory.
- Unless otherwise noted, enable the FTP server function on every router.

↘ Configuring a Top-Level Directory

- Mandatory.
- Unless otherwise noted, configure the top-level directory as the root directory on every router.

↘ Configuring a User Name and Password for Login

- Mandatory.
- The lengths of the user name and password are restricted.

↘ Configuring the Login Timeout for an FTP Session

- Optional.
- When the client is disconnected from the server due to an error or other abnormal causes, the FTP server may not know that the user is disconnected and continues to keep the connection. Consequently, the FTP connection is occupied for a long time and the server cannot respond to the login requests of other users. This configuration can ensure that other users can connect to the FTP server within a period of time upon an error.

Verification

Connect an FTP client to the FTP server.

- Check whether the client is connected.
- Check whether operations on the client are normal.

Related Commands

Enabling the FTP Server Function

Command	**ftp-server enable**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	The client cannot access the FTP server unless the top-level directory, user name and password are configured. Therefore, it is recommended that you configure the top-level directory, user name and password for login by referring to the subsequent chapters before enabling the service for the first time.

Configuring the Valid Login Count

Command	**ftp-server login times** *times*
Parameter Description	*times:* Indicates the valid login count, ranging from 1 to 10.
Command Mode	Global configuration mode
Usage Guide	The valid login count refers to the number of times you can perform account verification during an FTP session. The default value is 3, which means that your session will be terminated if you enter an incorrect user name or password for three times and other users can go online.

Configuring the Login Timeout for an FTP Session

Command	**ftp-server login timeout** *timeout*
Parameter Description	*timeout*: Indicates the login timeout, ranging from 1 to 30 minutes.
Command Mode	Global configuration mode
Usage Guide	The login timeout refers to the maximum duration that the session lasts since being established. If you do not pass the password verification again during the login timeout, the session will be terminated to ensure that other users can log in.

Configuring the Top-Level Directory of the FTP Server

Command	**ftp-server topdir** *directory*

Parameter Description	*directory*: Indicates the user access path.
Command Mode	Global configuration mode
Usage Guide	If the top-level directory of the server is set to "/syslog", the FTP client can access only the files and directories in the "/syslog" directory on the device after login. Due to restriction on the top-level directory, the client cannot return to the upper directory of "/syslog".

Configuring a User Name and Password for Server Login

Command	**ftp-server username** *username* **password** [*type*] *password*
Parameter Description	***username***: Indicates a user name. *type*: 0 or 7. 0 indicates that the password is not encrypted (plaintext) and 7 indicates that the password is encrypted (cipher text). **password**: Indicates a password.
Command Mode	Global configuration mode
Usage Guide	The FTP server does not support anonymous login; therefore, a user name must be configured. A user name consists of up to 64 characters including letters, half-width digits and symbols without spaces. A password consists of only letters or digits. Spaces at the beginning and end of the password are ignored. Spaces inside the password are viewed as part of the password. A plaintext password consists of 1 to 25 characters. A cipher text password consists of 4 to 52 characters. User names and passwords must match. A maximum of 10 users can be configured.

Configuring the Idle Timeout for an FTP Session

Command	**ftp-server timeout** *time*
Parameter Description	*time*: Indicates the idle timeout, ranging from 1 to 3,600 minutes.
Command Mode	Global configuration mode
Usage Guide	The idle timeout of a session refers to the duration from the end of an FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command operation (for example, after a file is completely transferred), the server starts to count the idle time again, and stops when the next FTP client command operation arrives. Therefore, the configuration of the idle timeout has no effect on some time-consuming file transfer operations.

Displaying Server Status

Command	**show ftp-server**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display FTP server status.

Debugging

Command	**debug ftp-server pro/err**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to debug message/error events of the FTP server.

Configuration Example

Creating an FTP Server on an IPv4 Network

Scenario	• A TCP connection is established for transmission from a server to a client.
Configuration Steps	• Enable the FTP server function. • Configure the top-level directory/syslog. • Set the user name **user** and password to **password**. • Set the session idle timeout to 5 minutes. • Specify an AAA method.
	Hostname(config)#ftp-server username user Hostname(config)#ftp-server password password Hostname(config)#ftp-server timeout 5 Hostname(config)#ftp-server topdir / Hostname(config)#ftp-server enable Hostname(config)# ftp-server authentication name
Verification	Run the **show ftp-server** command to check whether the configuration takes effect.
	Hostname#show ftp-server ftp-server information ========== enable : Y topdir : tmp:/ timeout: 10min username:aaaa password:(PLAINT)bbbb connect num[2] [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21] client IP:192.168.21.26[3927] [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21] client IP:192.168.21.26[3929] username:a1 password:(PLAINT)bbbb connect num[0]

	username:a2	password:(PLAINT)bbbb	connect num[0]
	username:a3	password:(PLAINT)bbbb	connect num[0]
	username:a4	password:(PLAINT)bbbb	connect num[0]
	username:a5	password:(PLAINT)bbbb	connect num[0]
	username:a6	password:(PLAINT)bbbb	connect num[0]
	username:a7	password:(PLAINT)bbbb	connect num[0]
	username:a8	password:(PLAINT)bbbb	connect num[0]
	username:a9	password:(PLAINT)bbbb	connect num[0]

Common Errors

- No user name is configured.
- No password is configured.
- No top-level directory is configured.

1.5 Monitoring

Displaying

Description	Command
Displays the FTP server configuration.	**show ftp-server**

Debugging

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

Description	Command
Debugs the FTP server error events.	**debug ftp-server err**
Debugs the FTP server message events.	**debug ftp-server pro**

1 Configuring FTP Client

1.1 Overview

The File Transfer Protocol (FTP) is an application of TCP/IP. By establishing a connection-oriented and reliable TCP connection between the FTP client and server, a user can access a remote computer that runs the FTP server program.

An FTP client enables file transfer between a device and the FTP server over the FTP protocol. A user uses the client to send a command to the server. The server responds to the command and sends the execution result to the client. By means of command interaction, the user can view files in the server directory, copy files from a remote computer to a local computer, or transfer local files to a remote computer.

FTP is intended to facilitate sharing of program/data files and encourage remote operation (by using programs). Users do not need to be concerned with differences of different files systems on different hosts. Data is transmitted in an efficient and reliable manner. FTP enables remote file operation securely.

FTP clients are different from standard FTP clients that run interactive commands. Instead, you enter the **copy** command in CLI to perform control-connection instructions such as **open**, **user**, and **pass**. After a control connection is established, the file transfer process starts, and then a data connection is established to upload or download files.

Old devices support TFTP. However, TFTP is used to transfer small files whereas FTP is used to transfer large files. Implementing FTP on a device enables the file transfer between the local device and other clients or servers.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)

1.2 Applications

Application	Description
Uploading a Local File to a Remote Server	Local and remote files need to be shared, for example, uploading a local file to a remote server.
Downloading a File from a Remote Server to a Local Device	Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

1.2.1 Uploading a Local File to a Remote Server

Scenario

Local and remote files need to be shared, for example, uploading a local file to a remote server.

As shown in Figure 1-1, resources are shared only on the Intranet.

Figure 1-1



Deployment

- Implement only communication on the Intranet.
- Enable file uploading on the FTP client.
- Enable file uploading on the FTP server.

1.2.2 Downloading a File from a Remote Server to a Local Device

Scenario

Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

As shown in Figure 1-2, resources are shared only on the Intranet.

Figure 1-2



Deployment

- Implement only communication on the Intranet.
- Enable file downloading on the FTP client.
- Enable file downloading on the FTP server.

1.3 Features

Basic Concepts

Uploading FTP Files

Upload files from an FTP client to an FTP server.

Downloading FTP Files

Download files from an FTP server to an FTP client.

FTP Connection Mode

An FTP client and an FTP server can be connected in the active or passive mode.

FTP Transmission Mode

The transmission between an FTP client and an FTP server is available in two modes, namely, text (ASCII) and binary (Binary).

Specifying the Source Interface IP Address for FTP Transmission

An FTP client is configured with a source IP address for communication with an FTP server.

Overview

Feature	Description
Uploading FTP Files	Uploads files from an FTP client to an FTP server.
Downloading FTP Files	Downloads files from an FTP server to an FTP client.
FTP Connection Mode	Specifies the connection mode between an FTP client and an FTP server.
FTP Transmission Mode	Specifies the transmission mode between an FTP client and an FTP server.
Specifying the Source Interface IP Address for FTP Transmission	Configures a source IP address of an FTP client for communication with an FTP server.
Disabling Size Check of Files Downloaded from an FTP Server.	Disabling size check of files downloaded from an FTP server.

1.3.1 Uploading FTP Files

FTP enables file uploading. Start the FTP client and FTP server simultaneously, and upload files from the FTP client to the FTP server.

1.3.2 Downloading FTP Files

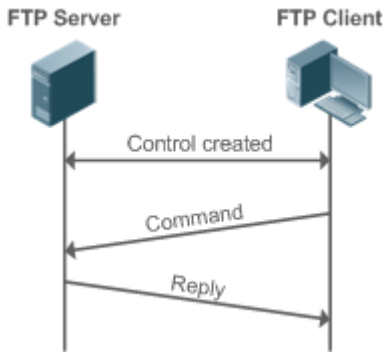
FTP enables file downloading. Start the FTP client and FTP server simultaneously, and download files from the FTP server to the FTP client.

1.3.3 FTP Connection Mode

FTP needs to use two TCP connections: one is a control link (command link) that is used to transfer commands between the FTP client and server; the other one is a data link that is used to upload or download data.

1. Control connection: Some simple sessions are enabled with the control connection only. A client sends a command to a server. After receiving the command, the server sends a response. The process is shown in Figure 1-3.

Figure 1-3 Control Connection



2. Control connection and data connection: When a client sends a command for uploading or downloading data, both the control connection and data connection need to be established.

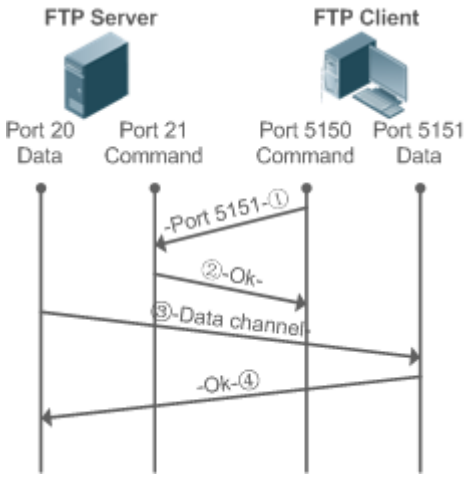
FTP supports two data connection modes: active (PORT) and passive (PASC). The two modes are different in establishing a data connection.

- Active mode

In this mode, an FTP server connects to an FTP client actively when a data connection is established. This mode comprises four steps:

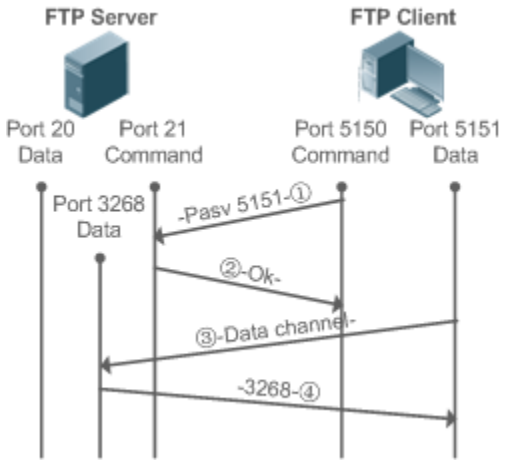
1. The client uses source port 5150 to communicate with the server through port 21, as shown in Figure 1-4, to send a connection request and tell the server that the port to be used is port 5151.
2. After receiving the request, the server sends a response OK(ACK). The client and server exchanges control signaling by console ports.
3. The server enables port 20 as the source port to send data to port 5151 of the client.
4. The client sends a response. Data transmission ends.

Figure 1-4 Active (PORT) Mode



- Passive mode

Figure 1-5 Passive (PASV) Mode



This mode is often set by the **passive** command. When a data connection is established, the FTP server is connected to the FPT client passively. This mode comprises four steps:

1. In the passive mode, the client initializes the control signaling connection. The client uses source port 5150 to connect to the server through port 21, and runs the **passive** command to request the server to enter the PASV mode.
2. The server agrees to enter the PASV mode, selects a port number greater than 1024 at random, and tells the port number to the client.
3. After receiving the message, the client uses port 5151, as shown in Figure 1-5, to communicate with the server through port 3268. Here, port 5151 is the source port and port 3268 is the destination port.
4. After receiving the message, the server sends data and responds an ACK(OK) response.

After the data connection is established, you can perform file uploading and downloading. Besides, you can perform some operations on the server file from the client.

The control connection for command and feedback transmission is always present whereas the data connection is established as required. Only an FTP client has the right to select and set the PASV or PORT mode. The FTP client sends a command to establish a data connection. FTP clients use the PASV mode by default.

1.3.4 FTP Transmission Mode

FTP provides two transmission modes: text (ASCII) and binary (Binary). At present, FTP clients support both the ASCII and Binary modes and use the BINARY mode by default.

- ASCII mode

The difference between the ASCII and Binary modes lies in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to a local Carriage Return Character (CRC), for example, \n in Unix, \r\n in Windows, and \r in Mac.

- Binary mode

The Binary mode can be used to transfer executable files, compressed files and image files without processing data. For example, a text file needs to be transferred from Unix to Windows. When the Binary mode is used, the line breaks in Unix will not be converted from \r to \r\n; therefore in Windows, this file has no line feeds and displays many black squares. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

1.3.5 Specifying the Source Interface IP Address for FTP Transmission

An FTP client is configured with a source IP address for communication with an FTP server. In this way, the FTP client connects to the server and shares files with the server through the specified source IP address.

1.3.6 Disabling Size Check of Files Downloaded from an FTP Server.

By disabling file size check, you can download files from FTP servers that cannot reply file size to FTP clients.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	⚠ (Mandatory) It is used to configure the functions of an FTP client.	
	copy flash	Uploads a file.
	copy ftp	Downloads a file.
Configuring Optional Functions	⚠ (Optional) It is used to configure the working mode of the FTP client.	
	ftp-client port	Sets the connection mode to active (port).
	ftp-client ascii	Sets the transmission mode to ASCII.
	ftp-client source-address	Configures the source IP address of the FTP client.
	default ftp-client	Restores the default settings, namely, connection mode set to passive (PASV), transmission mode to Binary and source IP address removed.
	ftp-client disable-size-check	Disables size check of FTP files.

1.4.1 Configuring Basic Functions

Configuration Effect

- Implement file uploading and downloading.

Notes

- Pay attention to the command formats for uploading and downloading.

Configuration Steps

↘ Uploading a File

- This configuration is mandatory when a file needs to be uploaded.
- Configure the FTP URL as the destination address of **copy** in Privileged EXEC mode.

↘ Downloading a File

- This configuration is mandatory when a file needs to be downloaded.
- Configure the FTP URL as the source address of **copy** in Privileged EXEC mode.

Verification

- Check whether the uploaded file exists on the FTP server.
- Check whether the downloaded file exists at the destination address.

Related Commands

Uploading a File

Command	**copy flash:**[*local-directory/*]*local-file* **ftp:** *//username:password@dest-address*[*/remote-directory*]*/remote-file*
Parameter Description	*local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory. *local-file:* Specifies a local file to be uploaded. *username*: Specifies a user name for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as "/", ":" and space. This parameter is mandatory. *password:* Specifies a password for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as "/", ":" and space. This parameter is mandatory. *dest-address:* Specifies an IP address for the FTP server. *remote-directory:* Specifies a directory on the server. *remote-file:* Renames the file on the server. ⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to upload a file from the flash of a local device to an FTP server.

Downloading an FTP File

Command	**copy ftp:***//username:password@dest-address*[*/remote-directory*]*/remote-file* **flash:**[*local-directory/*]*local-file*
Parameter Description	*username*: Specifies a user name for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as "/", ":" and space. This parameter is mandatory. *password:* Specifies a password for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as "/", ":" and space. This parameter is mandatory. *dest-address:* Specifies an IP address for the FTP server. *remote-directory:* Specifies a directory on the server. *remote-file:* Specifies a file to be downloaded. *local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory. *local-file:* Renames the file in the local flash. ⚠ The directory specified by the *local-directory* field must have been created on the device. This

	command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to download a file from an FTP server to the flash of a local device.

Configuration Example

↘ Uploading a File

Configuration Steps	Upload the **local-file** file in the **home** directory of a device to the **root** directory of an FTP server whose user name is **user**, password is **pass** and IP address is **192.168.23.69** and name the file as **remote-file**.
	Hostname# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file
Verification	Check whether the **remote-file** file exists on the FTP server.

↘ Downloading a File

Configuration Steps	Download the **remote-file** file from the **root** directory of an FTP server whose user name is **user**, password is **pass** and IP address is **192.168.23.69** to the **home** directory of a device and save the file as **local-file**.
	Hostname# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file
Verification	Check whether the **remote-file** file exists in the **home** directory of the flash.

Common Errors

- The command formats for uploading and downloading are incorrect.
- The user name or password is incorrect.

1.4.2 Configuring Optional Functions

Configuration Effect

- Set the connection and transmission modes and configure a source IP address of the client for file uploading and download.

Notes

- If an FTP client needs to be configured based on VRF, specify a VRF first.

Configuration Steps

↘ Setting the Connection Mode to Active (Port)

- Optional.
- Configure the connection mode of FTP.

Setting the Transmission Mode to ASCII

- Optional.
- Configure the transmission mode of FTP.

Configuring the Source IP Address of the FTP Client

- Optional.
- Configure the source IP address of the FTP client.

The version of configuring commands on the source port is supported. In the global configuration mode, the version provides the **ftp client source** command to configure the source interface IP address and the source IP address. The original **ftp client soure-address** command is abandoned and hidden. But if a user runs this original command, it is identified as a new configuration command and is saved.

Restoring the Default Settings

- Optional.
- Restore the default settings of the FTP client.

Verification

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

Related Commands

Setting the Connection Mode to Active (Port)

Command	**ftp-client** [**vrf** *vrf-name*] **port** **ftp-client port**
Parameter Description	**vrf** *vrf-name*: Specifies a VRF.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the connection mode to active (port). The default connection mode is passive (PASV).

Configuring the Source IP Address of the FTP Client

Command	**ftp-client** [**vrf** *vrfname*] **source** {*ip-address* | *ipv6-address* | *interface*} **ftp-client** [**vrf** *vrfname*] **source** {*ip-address* | *interface*} **ftp-client source** {*ip-address* | *ipv6-address* | *interface*} **ftp-client source** {*ip-address* | *interface*} **ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6-address* } **ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* } **ftp-client source-address** {*ip-address* | *ipv6-address* } **ftp-client source** {*ip-address* | *interface*}
Parameter Description	**vrf** *vrf-name*: Specifies a VRF. *ip-address:* Specifies the IPv4 address of a local interface.

	ipv6-address: Specifies the IPv6 address of a local interface. *Interface*: Specifies a source interface of a client.
Command Mode	Global configuration mode
Usage Guide	This command replaces the **ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6-address*} command to configure the source interface IP address and the source IP address. When run, this **ftp-client** [**vrf** *vrfname*] **source-address** {*ip-address* | *ipv6-address*} command is identified as a new command and is saved. Run this command to configure an interface IP address of the client for connection to the server. By default, the client is not configured with a local IP address. Instead, the route selects an IP address for the client.

Setting the Transmission Mode to ASCII

Command	**ftp-client** [**vrf** *vrf-name*] **ascii** **ftp-client ascii**
Parameter Description	**vrf** *vrf-name*: Specifies a VRF.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the transmission mode to ASCII. The default transmission mode is Binary.

Restoring the Default Settings

Command	**default ftp-client** [**vrf** *vrf-name*] **default ftp-client**
Parameter Description	**vrf** *vrf-name*: Specifies a VRF.
Command Mode	Global configuration mode
Usage Guide	Run this command to restore the default settings, namely, connection mode set to passive (PASV), transmission mode to Binary and source IP address removed.

Disabling Size Check of FTP Files

Command	**ftp-client disable-size-check**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to disable size check of FTP files downloaded from an FTP server.

Configuration Example

Configuring Optional Functions

Configuratio	● Set the connection mode of FTP to port.

n Steps	• Set the transmission mode to ASCII. • Set the source IP address to 192.168.23.167. • Set the connection mode of vrf 123 to port. • Set the transmission mode of vrf 123 to ASCII.
	Hostname# configure terminal Hostname(config)# ftp-client ascii Hostname(config)# ftp-client port Hostname(config)# ftp-client source-address 192.168.23.167 Hostname(config)# ftp-client vrf 123 port Hostname(config)# ftp-client vrf 123 ascii Hostname(config)# end
Verification	Run the **show run** command on the device to check whether the configuration takes effect. Hostname# show run ! ftp-client ascii ftp-client port ftp-client vrf 123 port ftp-client vrf 123 ascii ftp-client source-address 192.168.23.167 !

Common Errors

- The source IP address is not a local IP address.
- Before configuring the **ftp-client vrf** command, configure the **vrf** command.

1.5 Monitoring

Displaying

Description	Command
Displays the FTP client configuration.	**show run**

Debugging

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

Description	Command
Debugs the FTP Client.	**debug ftp-client**

1 Configuring TFTP Client

1.1 Overview

Trivial File Transfer Protocol (TFTP) is a specific application of Transmission Control Protocol/Internet Protocol (TCP/IP). File transfer between the TFTP client and server is implemented based on User Datagram Protocol (UDP). Compared with the TCP-based FTP protocol, TFTP does not require authentication or have complex packets. It is suitable for a stable network environment.

TFTP is used for small file transfer, and FTP supports transfer of large files.

Protocols and Standards

- RFC783: Trivial FILE TRANSFER PROTOCOL (TFTP)

1.2 Applications

Application	Description
Uploading a File from a Local Device to the remote TFTP server	A local device needs to upload a file to the remote TFTP server.
Downloading a File from the Remote TFTP Server to a Local Device	A local device needs to download a file from the remote TFTP server.

1.2.1 Uploading a File from a Local Device to the remote TFTP server

Scenario

A local device needs to upload a file to the remote TFTP server.

As shown in the following figure, resource sharing is provided only on the Intranet.

Figure 1-1



Deployment

- Only communication is implemented on the Intranet.
- Enable the TFTP client file upload function on the TFTP client.

- Enable the TFTP server file upload function on the TFTP server.

1.2.2 Downloading a File from the Remote TFTP Server to a Local Device

Scenario

A local device needs to download a file from the remote TFTP server.

As shown in the following figure, resource sharing is provided only on the Intranet.

Figure 1-2



Deployment

- Only communication is implemented on the Intranet.
- Enable the TFTP client file download function on the TFTP client.
- Enable the TFTP server file download function on the TFTP server.

1.3 Features

Basic Concepts

Uploading a File Using TFTP

Upload a file from the TFTP client to the TFTP server.

Downloading a File Using TFTP

Download a file from the TFTP server to the TFTP client.

Specifying the Source Interface IP Address for TFTP Transmission

Specify the source IP address for the TFTP client to communicate with the TFTP server.

Specifying the Port Number for Connection with the TFTP Server

Specify the port used by the TFTP client to communicate with the TFTP server.

Overview

Feature	Description
Uploading a File Using TFTP	Upload a file from the TFTP client to the TFTP server.
Downloading a File Using TFTP	Download a file from the TFTP server to the TFTP client.

Specifying the Source Interface IP Address for TFTP Transmission	Specify the source IP address for the TFTP client to communicate with the TFTP server.
Specifying the Port Number for Connection with the TFTP Server	Specify the port used by the TFTP client to communicate with the TFTP server.

1.3.1 Uploading a File Using TFTP

TFTP has the file upload function. To upload a file using TFTP, enable the file upload function on both the TFTP client and TFTP server and upload a file from the TFTP client to the TFTP server.

1.3.2 Downloading a File Using TFTP

TFTP has the file download function. To download a file using TFTP, enable the file download function on both the TFTP client and TFTP server and download a file from the TFTP server to the TFTP client.

1.3.3 Specifying the Source Interface IP Address for TFTP Transmission

You can configure the source IP address for the TFTP client to connect with and share files with the TFTP server.

1.3.4 Specifying the Port Number for Connection with the TFTP Server

You can specify the port number for the TFTP client to connect with and share files with the TFTP server.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic TFTP Client Functions	⚠ (Mandatory) It is used to configure the TFTP client functions.	
	copy flash	Uploads a file.
	copy tftp	Downloads a file.
Configuring Optional TFTP Client Functions	⚠ (Optional) It is used to configure the working mode of the TFTP client.	
	tftp-client source	Configures the source IP address of the TFTP client used for the TFTP connection.
	tftp-client port	Configures the port number used by the TFTP client to connect with the TFTP server.

1.4.1 Configuring Basic TFTP Client Functions

Configuration Effect

- Implement file upload and download.

Notes

- Note the format of files to be uploaded or downloaded.

Configuration Steps

Uploading a File

- Mandatory.
- Configure the TFTP-related Uniform Resource Locators (URLs) for the destination address under copy in privileged EXEC mode.

Downloading a File

- Mandatory.
- Configure the TFTP-related URLs for the source address under copy in privileged EXEC mode.

Verification

- Check whether the uploaded file exists in a directory of the TFTP server.
- Check whether the downloaded file exists in the destination address.

Related Commands

Uploading a File

Command	**copy flash:**[local-directory/]local-file **tftp:** // dest-address[/remote-directory]/remote-file
Parameter Description	*local-directory*: Directory on the local device. If no directory is specified, the current directory is used. *local-file*: Name of the local file to be operated. *dest-address*: IP address of the TFTP server. *remote-directory*: Directory path on the TFTP server. *remote-file*: Name of the file to be operated on the TFTP server. ⚠ The directory specified by *local-directory* must already exist on the device. This command does not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	This command is used to upload a file in the **flash** directory of the local device to the TFTP server.

Downloading a File

Command	**copy tftp:**// dest-address[/remote-directory]/remote-file **flash:**[local-directory/]local-file
Parameter Description	*dest-address*: IP address of the TFTP server. *remote-directory*: Directory path on the TFTP server. *remote-file*: Name of the file to be operated on the TFTP server. *local-directory*: Directory on the local device. If no directory is specified, the current directory is used. *local-file*: Name of the local file to be operated. ⚠ The directory specified by *local-directory* must already exist on the device. This command does not

	automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	This command is used to download a file from the TFTP server to the **flash** directory of the local device.

Configuration Example

The following configuration example only describes configurations related to TFTP client upload and download.

Uploading a File

Configuration Steps	Upload the **local-file** file in the **flash** directory on the device to the **root** directory of the TFTP server whose IP address is 192.168.23.69 and rename the file as **remote-file**.
	Hostname# copy flash:local-file tftp://192.168.23.69/root/remote-file
Verification	Check whether the **remote-file** file exists on the TFTP server.

Downloading a File

Configuration Steps	Download the **remote-file** file from the **root** directory of the TFTP server whose IP address is 192.168.23.69 to the **flash** directory of the device and rename it as **local-file**.
	Hostname# copy tftp://192.168.23.69/root/remote-file flash:local-file
Verification	Check whether the **local-file** file exists in the **home** directory under the **flash** directory.

Common Errors

- The format of the uploaded or downloaded file is incorrect.
- The username or password is incorrect.

1.4.2 Configuring Optional TFTP Client Functions

Configuration Effect

- Download or upload files using the specified IP address and port number of the TFTP client.

Notes

- The remote port number ranges from 20000 to 65534.

Configuration Steps

Configuring the Source IP Address for TFTP Connection

- Optional.
- Configure the source IP address of the TFTP client used for the TFTP connection.

Configuring the Port Number Used by the TFTP Client to Connect with the TFTP Server

- Optional.
- Configure the port number used by the TFTP client to connect with the TFTP server.

Verification

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

Related Commands

Configuring the Source IP Address for the TFTP Connection

Command	**tftp-client source** { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }
Parameter Description	*ipv6*-address: IPv6 address of the local interface. *ip-address*: IPv4 address of the local interface.
Command Mode	Global configuration mode
Usage Guide	You can use this command to bind the TFTP client to the IP address of a port so that the TFTP can use this IP address to connect with the TFTP server. By default, no source IP address is bound to the TFTP client, and an IP address is selected for the client based on the route.

Configuring the Port Number Used by the TFTP Client to Connect with the TFTP Server

Command	**tftp-client port** *port-number*
Parameter Description	*port*-number: Port number.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the port number used by the TFTP client to connect with the TFTP server.

1.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays TFTP client configurations.	**show running-config**

Debugging

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

Description	Command
Debugs the TFTP client.	**debug tftp**

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_Managing_Network_Devices	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.

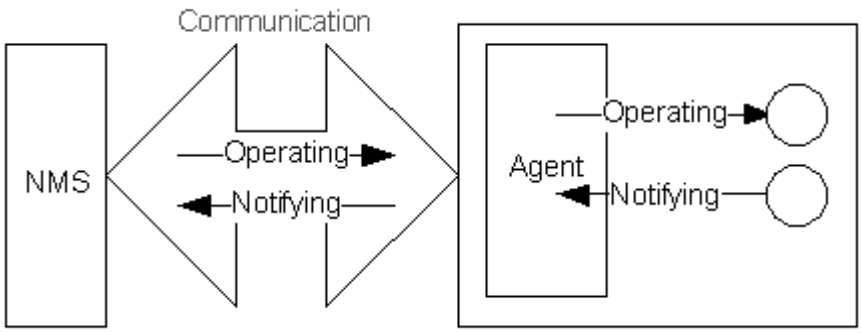
1.3 Features

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.

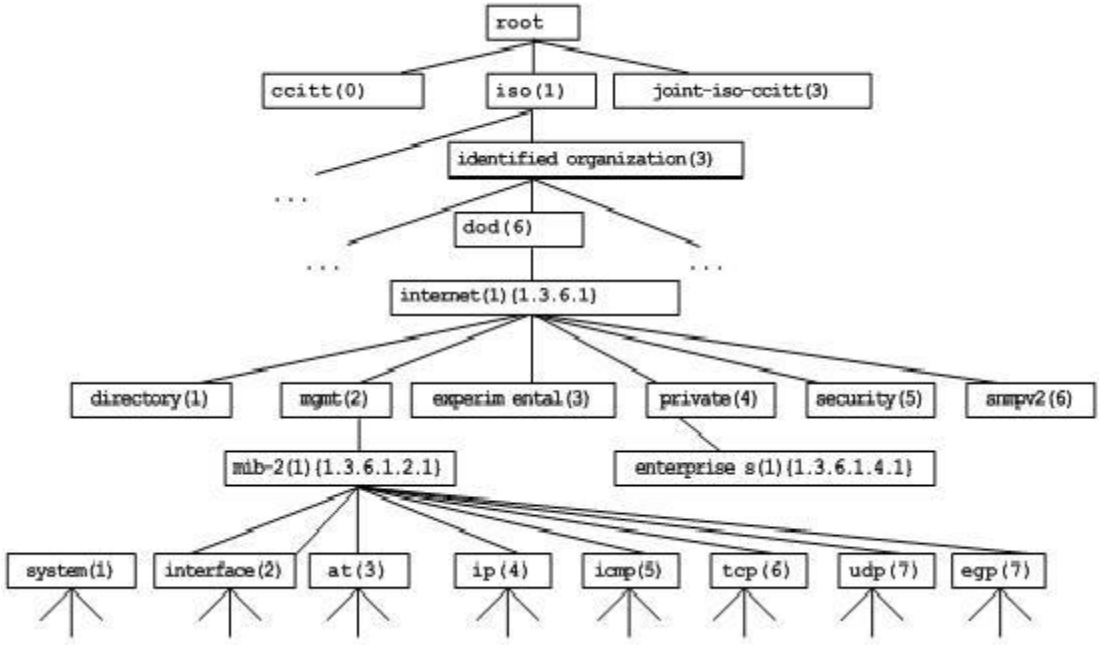
SNMP Agent

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



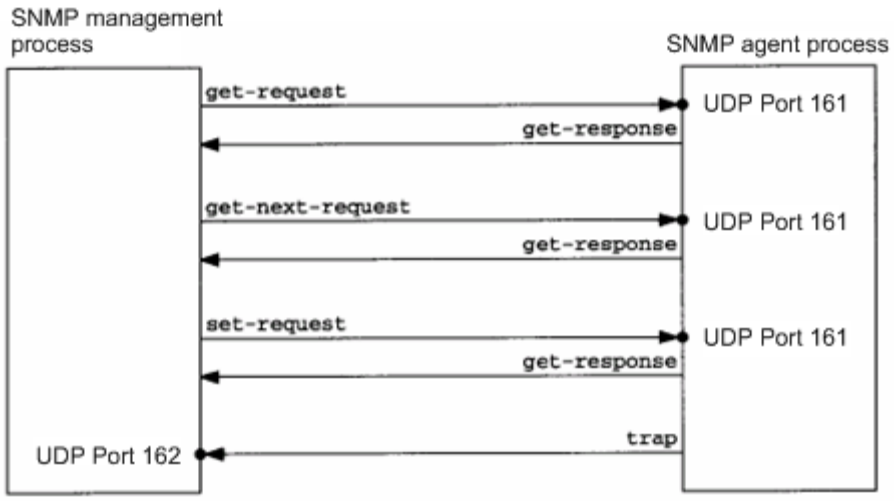
Operation Types

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, system location, and device Network Element (NE) information are empty. The default serial number is 60FF60, the default maximum packet length is 1,572 bytes, and the default UDP port ID of the SNMP service is 161.

The **snmp-server contact** command is used to configure or delete the system contact mode.

The **snmp-server location** command is used to configure or delete the system location.

The **snmp-server chassis-id** command is used to configure the system serial number or restore the default value.

The **snmp-server packetsize** command is used to configure the maximum packet length of the agent or restore the default value.

The **snmp-server net-id** command is used to configure or delete the device NE information.

The **snmp-server udp-port** command is used to set the UDP port ID of the SNMP service or restore the default value.

Configuring the SNMP Host Address

By default, no SNMP host is configured.

The **snmp-server host** command is used to configure the NMS host address to which the agent actively sends messages or to delete the specified SNMP host address. In the messages sent to the host, the SNMP version, receiving port, authentication name, or user can be bound. This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

Setting Trap Message Parameters

By default, SNMP is not allowed to actively send a trap message to the NMS, the function of sending a Link Trap message on an interface is enabled, the function of sending a system reboot trap message is disabled, and a trap message does not carry any private field.

By default, the IP address of the interface where SNMP packets are sent is used as the source address.

By default, the length of a trap message queue is 10 and the interval for sending a trap message is 30s.

The **snmp-server enable traps** command is used to enable or disable the agent to actively send a trap message to the NMS.

The **snmp trap link-status** command is used to enable or disable the function of sending a Link Trap message on an interface.

The **snmp-server trap-source** command is used to specify the source address for sending messages or to restore the default value.

The **snmp-server queue-length** command is used to set the length of a trap message queue or to restore the default value.

The **snmp-server trap-timeout** command is used to set the interval for sending a trap message or to restore the default value.

The **snmp-server trap-format private** command is used to set or disable the function of carrying private fields in a trap message when the message is sent.

The **snmp-server system-shutdown** command is used to enable or disable the function of sending a system reboot trap message.

Setting 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.

Setting the SNMP Attack Protection and Detection Function

By default, the SNMP attack protection and detection function is disabled.

The **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** } command is used to set and enable the attack protection and detection function.

Setting the SNMP Logging Function to Record the Get, Get-Next, and Set Operations Performed by the NMS on the SNMP Agent

By default, SNMP logging is enabled.

The **snmp-server logging** { **get-operation** | **set-operation** } command is used to enable the function of recording the Get and Set operations. **get-operation** controls the Get and Get-Next operations records, and **set-operation** controls the Set operation records.

Configuring the Heartbeat Trap Function and Interval

By default, the heartbeat trap function is enabled and heartbeat trap messages are sent at the interval of 5 minutes.

Run the **no snmp-server heartbeat on** command to disable the heartbeat trap function.

Run the **snmp-server heartbeat period** to configure the interval for sending heartbeat trap messages.

1.3.2 SNMPv1 and SNMPv2C

SNMPv1 and SNMPv2C adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

Working Principle

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. The authentication name of the NMS must be the same as an authentication name defined in devices.

SNMPv2C adds the Get-bulk operation mechanism and can return more detailed error message types to the management workstation. The Get-bulk operation is performed to obtain all information from a table or obtain lots of data at a time, so as to reduce the number of request responses. The enhanced error handling capabilities of SNMPv2C include extension of error codes to differentiate error types. In SNMPv1, however, only one error code is provided for errors. Now, errors can be differentiated based on error codes. Because management workstations supporting SNMPv1 and SNMPv2C may exist on the network, the SNMP agent must be able to identify SNMPv1 and SNMPv2C packets and return packets of the corresponding versions.

Security

One authentication name has the following attributes:

- Read-only: Provides the read permission of all MIB variables for authorized management workstations.
- Read-write: Provide the read/write permission of all MIB variables for authorized management workstations.

Related Configuration

Setting Authentication Names and Access Permissions

The default access permission of all authentication names is read-only.

The **snmp-server community** command is used to configure or delete an authentication name and access permission.

This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed.

1.3.3 SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2 into the SNMPv3 system.

Working Principle

The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications of SNMP, which work by using the services provided by the SNMP engine.

SNMPv3v determines whether a user has the right to use MIB objects by using the User-based Security Model (USM). The security level of the NMS user must be the same as that of an SNMP user defined in devices so as to manage devices.

SNMPv3 requires the NMS to obtain the SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the discover and report operation mechanisms. When the NMS does not know agent engine IDs, the NMS may first send a discover message to the agent and the agent returns a report message carrying an engine ID. Later, management operations between the NMS and the agent must carry the engine ID.

Security

- SNMPv3 determines the data security mechanism based on the security model and security level. At present, security models include: SNMPv1, SNMPv2C, and SNMPv3. SNMPv3 includes SNMPv1 and SNMPv2C into the security model.

SNMPv1 and SNMPv2C Security Models and Security Levels

Security Model	Security Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.
SNMPv2c	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.

SNMPv3 Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User name.	N/A	Data validity is confirmed through user name.
SNMPv3	authNoPriv	MD5 or SHA	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5 or SHA	DES	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA and data encryption mechanism based on CBC-DES are provided.

Engine ID

An engine ID is used to uniquely identify an SNMP engine. Because each SNMP entity includes only one SNMP engine, one SNMP engine uniquely identifies an SNMP entity in a management domain. Therefore, the SNMPv3 agent as an entity must has a unique engine ID, that is, SnmpEngineID.

An engine ID is an octet string that consists of 5 to 32 bytes. RFC3411 defines the format of an engine ID:

- The first four bytes indicate the private enterprise ID (allocated by IANA) of a vendor, which is expressed in hexadecimal.
- The fifth byte indicates remaining bytes:
- 0: Reserved.
- 1: The later four bytes indicate an IPv4 address.
- 2: The later 16 bytes indicate an IPv6 address.
- 3: The later six bytes indicate a MAC address.
- 4: Text consisting of 27 bytes, which is defined by the vendor.
- 5: Hexadecimal value consisting of 27 bytes, which is defined by the vendor.

- 6-127: Reserved.
- 128-255: Formats specified by the vendor.

Related Configuration

Configuring an MIB View and a Group

By default, one view is configured and all MIB objects can be accessed.

By default, no user group is configured.

The **snmp-server view** command is used to configure or delete a view and the **snmp-server group** command is used to configure or delete a user group.

One or more instructions can be configured to specify different community names so that network devices can be managed by NMSs of different permissions.

Configuring an SNMP User

By default, no user is configured.

The **snmp-server user** command is used to configure or delete a user.

The NMS can communicate with the agent by using only legal users.

An SNMPv3 user can specify the security level (whether authentication and encryption are required), authentication algorithm (MD5 or SHA), authentication password, encryption password (only DES is available currently), and encryption password.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic SNMP Functions	⚠ (Mandatory) It is used to enable users to access the agent through the NMS.	
	enable service snmp-agent	Enables the agent function.
	snmp-server community	Sets an authentication name and access permission.
	snmp-server user	Configures an SNMP user.
	snmp-server view	Configures an SNMP view.
	snmp-server group	Configures an SNMP user group.
	snmp-server authentication	Configures the SNMP attack protection and detection function.
	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.

Configuration	Description and Command	
	snmp trap link-status	Enables the function of sending a Link Trap message on an interface.
	snmp-server system-shutdown	Enables the function of sending a system reboot trap message.
	snmp-server trap-source	Specifies the source address for sending a trap message.
	snmp-server trap-format private	Enables a trap message to carry private fields when the message is sent.
	snmp-server inform	Configuring the Inform Retry Times and Request Timeout Interval.
	snmp-server heartbeat	Configures the heartbeat trap function and interval.
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.
	no enable service snmp-agent	Disabling the SNMP Agent Function for the Device
Setting SNMP Control Parameters	⚠ (Optional) It is used to set or modify SNMP control parameters.	
	snmp-server contact	Sets the device contact mode.
	snmp-server location	Sets the device location.
	snmp-server logging	Sets the logging function.
	snmp-server chassis-id	Sets the serial number of the device.
	snmp-server net-id	Sets NE information about the device.
	snmp-server packetsize	Modifies the maximum packet length.
	snmp-server udp-port	Modifies the UDP port ID of the SNMP service.
	snmp-server queue-length	Modifies the length of a trap message queue.
	snmp-server trap-timeout	Modifies the interval for sending a trap message.

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.

Verification

Run the **show snmp** command to check the SNMP function on devices.

Related Commands

Configuring an SNMP View

Command	**snmp-server view** *view-name oid-tree* { **include** | **exclude** }
Parameter Description	*view-name*: View name *oid-tree*: MIB objects associated with a view, which are displayed as an MIB subtree. **include:** Indicates that the MIB object subtree is included in the view. **exclude:** Indicates that the MIB object subtree is not included in the view.
Command Mode	Global configuration mode
Usage Guide	Specify a view name and use it for view-based management.

Configuring an SNMP User Group

Command	**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { [**ipv6** *ipv6-aclname*] *aclnum* | *aclname* }]
Parameter Description	**v1** | **v2c** |**v3:** Specifies the SNMP version. **auth:** Messages sent by users in the group need to be verified but data confidentiality is not required. This configuration is valid for SNMPv3 only. **noauth:** Messages sent by users in the group do not need to be verified and data confidentiality is not required. This configuration is valid for SNMPv3 only. **priv:** Messages sent by users in the group need to be verified and confidentiality of transmitted data is required. This configuration is valid for SNMPv3 only. *readview*: Associates one read-only view. *writeview*: Associates one read/write view. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Associate certain users with a group and associate the group with a view. Users in a group have the same access permission. In this way, you can determine whether managed objects associated with an operation are in the allowable range of a view. Only managed objects in the range of a view can be accessed.

Configuring an Authentication Name and Access Permission

Command	**snmp-server community** [*0* | *7*] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]
Parameter Description	*0*: Indicates that the input community string is a plaintext string. *7*: Indicates that the input community string is a ciphertext string. *string*: Community string, which is equivalent to the communication password between the NMS and the SNMP agent. *view-name*: Specifies a view name for view-based management. **ro:** Indicates that the NMS can only read variables of the MIB. **rw:** The NMS can read and write variables of the MIB. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified. *ipaddr*: Associates NMS addresses and specifies NMS addresses for accessing the MIB.
Command Mode	Global configuration mode

Usage Guide	This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed. To disable the SNMP agent function, run the **no snmp-server** command.

Configuring an SNMP User

Command	**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { [**ipv6** *ipv6-aclname*] *aclnum* | *aclname* }]
Parameter Description	*username*: User name. *groupname*: Specifies the group name for a user. **v1** | **v2c** | **v3:** Specifies the SNMP version. Only SNMPv3 supports later security parameters. **encrypted:** The specified password input mode is ciphertext input. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 protocol authentication key consists of 16 bytes and an SHA authentication protocol key consists of 20 bytes. Two characters stand for one byte. Encrypted keys are valid for this engine only. **auth:** Specifies whether authentication is used. **md5:** Specifies the MD5 authentication protocol. **sha** specifies the SHA authentication protocol. *auth-password*: Configures a password string (not more than 32 characters) used by the authentication protocol. The system converts the passwords into the corresponding authentication keys. **priv:** Specifies whether confidentiality is used. **des56** specifies the use of the 56-bit DES encryption protocol. *priv-password*: Configures a password string (not more than 32 characters) used for encryption. The system converts the password into the corresponding encryption key. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Configure user information so that the NMS can communicate with the agent by using a valid user. For an SNMPv3 user, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (at present, only DES is available), and encryption password.

Enabling the Agent Function

Command	**enable service snmp-agent**
Parameter Description	
Configuration mode	Privileged mode.
Usage Guide	This command is used to enable the SNMP agent function of a device.

Setting Password Dictionary Check for Communities and Users

Command	**snmp-server enable secret-dictionary-check**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	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. To disable password dictionary check, run the **no snmp-server enable secret-dictionary-check** command.

Enabling the SNMP Attack Protection and Detection Function

Command	**snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }
Parameter Description	*times*: Number of continuous failed attempts. **lock:** After continuous authentication fails, the source IP address is permanently forbidden to initiate authentication for access. The administrator needs to manually unlock the IP address. **lock-time** *minutes*: After continuous authentication fails, the source IP address is forbidden to initiate authentication for access in a period of time. Beyond the period, the source IP address can be authenticated for access again. **unlock:** After continuous authentication fails, the source IP address is allowed to access the MIB continuously, which is equivalent to the fact that the SNMP attack protection and detection function is not configured.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP attack protection and detection function so that the corresponding measure can be taken after continuous authentication fails. The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses. The source IP address that are forbidden to access the MIB in a period of time can be authenticated for access again after the period expires or after the administrator manually unlocks the IP addresses.

Setting the SNMP Logging Function to Record the Get, Get-Next, and Set Operations Performed by the NMS on the SNMP Agent

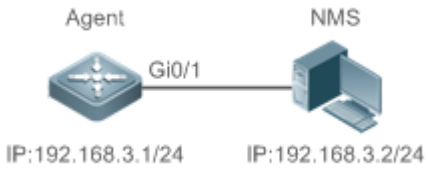
Command	**snmp-server logging** { **get-operation | set-operation** }
Parameter Description	g**et-operation:** Enables the logging of Get and Get-Next operations. **set-operation:** Enables the logging of the Set operation.
Command Mode	Global configuration mode
Usage Guide	This command is used to record the Get, Get-Next, and Set operations performed by the NMS on the SNMP agent. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value.

	⚠ A large number of logs will affect device performance. In normal conditions, you are advised to disable the SNMP logging function. Exercise caution when using the GET operation logging function; otherwise, spamming may occur due to a large number of requests.

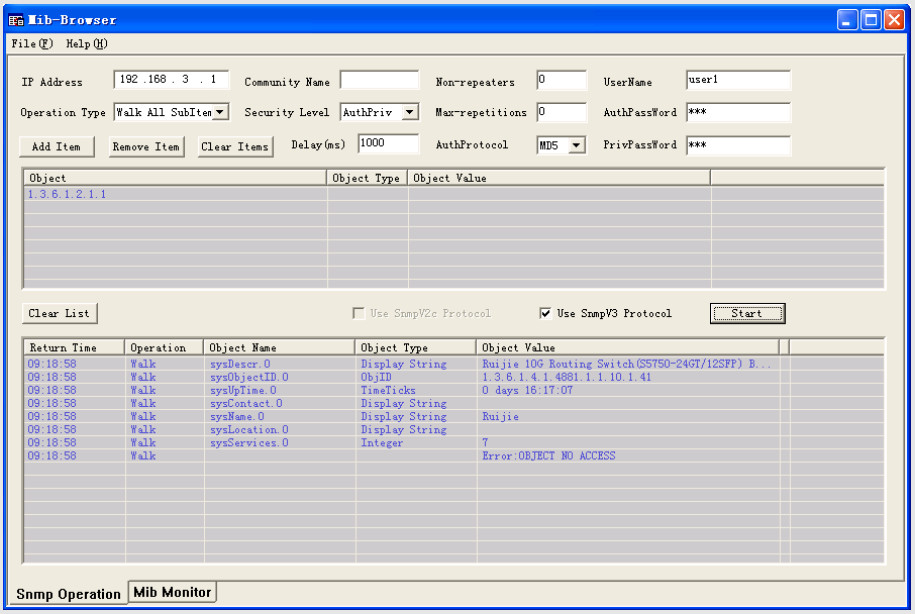
Displaying the SNMP Status Information

Command	**show snmp** [**mib** | **user** | **view** | **group**| **host** | **locked-ip** | **process-mib-time**]
Parameter Description	**mib:** Displays information about the SNMP MIB supported in the system. **user:** Displays information about an SNMP user. **view:** Displays information about an SNMP view. **group:** Displays information about an SNMP user group. **host:** Displays information about user configuration. **locked-ip:** Source IP address that is locked after continuous authentication fails. **process-mib-time:** Displays the MIB node with the longest processing time.
Configuration mode	Privileged mode.
Usage Guide	N/A

Configuring SNMPv3 Configuration

Scenario **Figure 1-5**	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● Network devices can control the operation permission of users to access MIB objects. For example, the user named user1 can read MIB objects under the system node (1.3.6.1.2.1.1) and can only write MIB objects under the SysContact node (1.3.6.1.2.1.1.4.0). ● Network devices can actively send authentication and encryption messages to the NMS.
Configuration Steps	● Configure a MIB view and a MIB group. Create a MIB view “view1”, which includes the associated MIB object (1.3.6.1.2.1.1); then create a MIB view “view2”, which includes the associated MIB object (1.3.6.1.2.1.1.4.0). Create a group “g1”, select the version “v3”, set the security level to the authentication and encryption mode “priv”, and configure permissions to read the view “view1” and write the view “view2”. ● Configure an SNMP user. Create a user named “user1” under group “g1”, select “v3” as the version, and set the authentication mode to “md5”, authentication password to “123”, encryption mode to “DES56”, and encryption password to “321”.

	● Configure the SNMP host address. Set the host address to 192.168.3.2, select "3" as the version, set the security level to the authentication and encryption mode "priv", and associate the user name "user1". Enable the agent to actively send a trap message to the NMS. ● Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	Hostname(config)#snmp-server view view1 1.3.6.1.2.1.1 include Hostname(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include Hostname(config)#snmp-server group g1 v3 priv read view1 write view2 Hostname(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 Hostname(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 Hostname(config)#snmp-server enable traps Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 Hostname(config-if-gigabitEthernet 0/1)#exit
Verification	1. Run the **show running-config** command to display configuration information of the device. 2. Run the **show snmp user** command to display the SNMP user. 3. Run the **show snmp view** command to display the SNMP view. 4. Run the **show snmp group** command to display the SNMP group. 5. Run the **show snmp host** command to display the host information configured by the user. 6. Install MIB-Browser.
Agent	Hostname# show running-config ! interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 ! snmp-server view view1 1.3.6.1.2.1.1 include snmp-server view view2 1.3.6.1.2.1.1.4.0 include snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56 D5CEC4884360373ABBF30AB170E42D03 snmp-server group g1 v3 priv read view1 write view2 snmp-server host 192.168.3.2 traps version 3 priv user1 snmp-server enable traps
	Hostname# show snmp user User name: user1 Engine ID: 800013110300d0f8221120 storage-type: permanent active Security level: auth priv Auth protocol: MD5 Priv protocol: DES Group-name: g1
	Hostname#show snmp view view1(include) 1.3.6.1.2.1.1 view2(include) 1.3.6.1.2.1.1.4.0

	default(include) 1.3.6.1
	Hostname# show snmp group groupname: g1 securityModel: v3 securityLevel:authPriv readview: view1 writeview: view2 notifyview:
	Hostname#show snmp host Notification host: 192.168.3.2 udp-port: 162 type: trap user: user1 security model: v3 authPriv
	Install MIB-Browser, enter IP address 1**92.168.3.1** 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.

Enabling a Trap Message to Carry Private Fields when the Message Is Sent

- Optional
- Configure this item on the agent when private fields need to be carried in a trap message.

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** { *host-addr* | **ipv6** *ipv6-addr* } [**traps | inrorms**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]
Parameter Description	*host-addr*: Address of the SNMP host. *ipv6-addr*: (IPv6) address of the SNMP host. **traps | informs:** Configures the host to send a trap message or an inform message. **version:** SNMP version, which can be set to **V1**, **V2C**, or **V3**. **auth** | **noauth** | **priv:** Sets the security level of V3 users. *community-string*: Community string or user name (V3). *port-num*: Configures the port ID of the SNMP host. *notification-type*: Type of trap messages that are actively sent, for example, snmp. If no trap type is specified, all trap messages are sent.
Command Mode	Global configuration mode
Usage Guide	This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS. You can configure different SNMP hosts to receive trap messages. A host can support different traps and ports. If the same host is configured, the last configuration is combined with the previous configurations, that is, to send different trap messages to the same host, configure one type of trap messages each time. These configurations are finally combined.

Enabling the Agent to Actively Send a Trap Message to the NMS

Command	**snmp-server enable traps** [*notification-type*]
Parameter Description	*notification-type*: Enables trap notification for the corresponding events, including the following types: authentication: Allow authentication notifications. snmp: SNMP trap message entity: entity Trap message. mac-notification: MAC trap message. nfpp: NFPP Traps message. web-auth: Web authentication trap message.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **snmp-server host** command to so that trap messages can be actively sent.

Enabling the Function of Sending a Link Trap Message on an Interface

Command	**snmp trap link-status**
Parameter Description	**-**
Configuration mode	Interface configuration mode

Usage Guide	For interfaces (Ethernet interface, AP interface, and SVI interface), when this function is enabled, the SNMP sends a Link Trap message if the link status on the interfaces changes. Otherwise, the SNMP does not send the message.

Enabling the Function of Sending a System Reboot Trap Message

Command	**snmp-server system-shutdown**
Parameter Description	-
Configuration mode	Global configuration mode
Usage Guide	When the function of notification upon SNMP system reboot is enabled, a trap message is sent to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

Command	**snmp-server trap-source** *interface*
Parameter Description	*interface*: Used as the interface for the SNMP source address.
Configuration mode	Global configuration mode
Usage Guide	By default, the IP address of the interface where SNMP packets are sent is used as the source address. To facilitate management and identification, this command can be run to permanently use one local IP address as the source SNMP address.

Enabling a Trap message to Carry Private Fields when the Message Is Sent

Command	**snmp-server trap-format private**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to enable a trap message to carry private fields when the message is sent. At present, supported private fields include the alarm generation time. For the specific data types and data ranges of the fields, see RUIJIE-TRAP-FORMAT-MIB.mib.

Configuring the Inform Retry Times and Request Timeout Interval

Command	**snmp-server inform** { **retries** *retry-time* | **timeout** *time* }
Parameter Description	*retry- time*: Specifies the retry times for inform requests, ranging from 0 to 255. *Time:* Specifies the inform request timeout interval, ranging from 0 to 21,474,836.
Configuration mode	Global configuration mode
Usage Guide	N/A

Configuring the Heartbeat Trap Function

Command	**snmp-server heartbeat on**

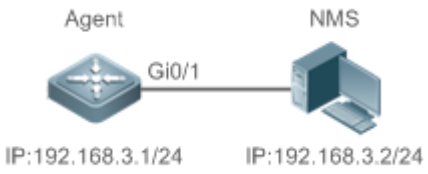
Parameter Description	N/A
Configuration Mode	Global configuration mode
Usage Guide	By default, the heartbeat trap function is enabled. You can run the **no snmp-server heartbeat** command to disable this function.

Configuring the Interval for Sending Heartbeat Trap Messages

Command	**snmp-server heartbeat period** *time*
Parameter Description	*time*: Indicates the interval (unit: second).
Configuration Mode	Global configuration mode
Usage Guide	This command configures the interval for sending heartbeat trap messages.

Configuration Example

Enabling the Trap Function

Scenario Figure 1-6	 ● The NMS manages network devices (agents) based on the community authentication mode, and network devices can actively send messages to the NMS.
Configuration Steps	1. Perform configuration to enable the agent to actively send messages to the NMS. Set the SNMP host address to 192.168.3.2, the message format to Version2c, and the authentication name to user1. Enable the agent to actively send trap messages. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	Hostname(config)#snmp-server host 192.168.3.2 traps version 2c user1 Hostname(config)#snmp-server enable traps Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 Hostname(config-if-gigabitEthernet 0/1)#exit
Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp** command to display the SNMP status.
Agent	Hostname# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0

	snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location fuzhou snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact ruijie.com.cn snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	Hostname#show snmp Chassis: 1234567890 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP global trap: enabled SNMP logging: disabled SNMP agent: enabled

Common Errors

N/A

1.4.3 Shielding the Agent Function

Configuration Effect

Shield the agent function when the agent service is not required.

Notes

- Run the **no snmp-server** command to shield the SNMP agent function when the agent service is not required.
- Different from the shielding command, after the **no enable service snmp-agent** command is run, all SNMP services are directly disabled (that is, the SNMP agent function is disabled, no packet is received, and no response packet or trap packet is sent), but configuration information of the agent is not shielded.

Configuration Steps

Shielding the SNMP Agent Function for the Device

- Optional
- To shield the configuration of all SNMP agent services, use this configuration.

Disabling the SNMP Agent Function for the Device

- Optional
- To directly disable all services, use this configuration.

Verification

Run the **show services** command to check whether SNMP services are enabled or disabled.

Run the **show snmp** command to display the SNMP status.

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

Related Commands

Shielding the SNMP Agent Function for the Device

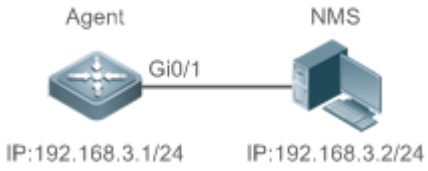
Command	**no snmp-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the SNMP agent function is disabled. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are set, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must also be run at the same time so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. Run the **no snmp-server** command to disable SNMP agent services of all versions supported by the device. After this command is run, all SNMP agent service configurations are shielded (that is, after the **show running-config** command is run, no configuration is displayed. Configurations are restored after the SNMP agent service is enabled again). After the **enable service snmp-agent** command is run, the SNMP agent configurations are not shielded.

Disabling the SNMP Agent Function for the Device

Command	**no enable service snmp-agent**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	disable the SNMP service, but it will not shield SNMP agent parameters.

Configuration Example

Enabling the SNMP Service

Scenario **Figure 1-7**	 After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.
Configuration Steps	1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	Hostname(config)#enable service snmp-agent
Verification	1. Run the **show services** command to check whether the SNMP service is enabled or disabled.
Agent	Hostname#show service web-server : disabled web-server(https): disabled snmp-agent : enabled ssh-server : disabled telnet-server : enabled

Common Errors

N/A

1.4.4 Setting SNMP Control Parameters

Configuration Effect

Set basic parameters of the SNMP agent, including the device contact mode, device location, serial number, and parameters for sending a trap message. By accessing the parameters, the NMS can obtain the contact person of the device and physical location of the device.

Notes

N/A

Configuration Steps

Setting the System Contact Mode

- Optional
- When the contact mode of the system needs to be modified, configure this item on the agent.

Setting the System Location

- Optional
- When the system location needs to be modified, configure this item on the agent.

Setting the System Serial Number

- Optional
- When the system serial number needs to be modified, configure this item on the agent.

Setting NE Information about the Device

- Optional
- When the NE code needs to be modified, configure this item on the agent.

Setting the Maximum Packet Length of the SNMP Agent

- Optional
- When the maximum packet length of the SNMP agent needs to be modified, configure this item on the agent.

Setting the UDP Port ID of the SNMP Service

- Optional
- When the UDP port ID of the SNMP service needs to be modified, configure this item on the agent.

Setting the Queue Length of Trap Messages

- Optional
- When the size of the message queue needs to be adjusted to control the message sending speed, configure this item on the agent.

Setting the Interval for Sending a Trap Message

- Optional
- When the interval for sending a trap message needs to be modified, configure this item on the agent.

Configuring SNMP Flow Control

- Optional
- If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Verification

Run the **show snmp** command to display the SNMP status.

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

Related Commands

Setting the System Contact Mode

Command	**snmp-server contact** *text*

Parameter Description	*text*: String that describes the system contact mode.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting the System Location

Command	**snmp-server location** *text*
Parameter Description	*text*: String that describes system information.
Configuration mode	Global configuration mode
Usage Guide	N/A

Setting the System Serial Number

Command	**snmp-server chassis-id** *text*
Parameter Description	*text*: Text of the system serial number, which 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 NE Information about the Device

Command	**snmp-server net-id** *text*
Parameter Description	*text*: Text that is used to set the device NE code. The text is a string that consists of 1 to 255 characters that are case-sensitive and may include spaces.
Configuration mode	Global mode.
Usage Guide	Set the NE code of the device.

Setting the Maximum Packet Length of the SNMP Agent

Command	**snmp-server packetsize** *byte-count*
Parameter Description	*byte-count*: Packet size, ranging from 484 bytes to 17,876 bytes.
Configuration mode	Global mode.
Usage Guide	N/A

Setting the UDP Port ID of the SNMP Service

Command	**snmp-server udp-port** *port-num*
Parameter Description	*port-num*: Specifies the UDP port ID of the SNMP service, that is, the ID of the protocol port that receives SNMP packets.

Configuration mode	Global mode.
Usage Guide	Specify the protocol port ID for receiving SNMP packets.

Setting the Length of a Trap Message Queue

Command	**snmp-server queue-length** *length*
Parameter Description	*length*: Queue length, ranging from 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the size of the message queue to control the message sending speed.

Setting the Interval for Sending a Trap Message

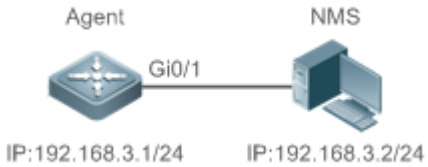
Command	**snmp-server trap-timeout** *seconds*
Parameter Description	*seconds*: Interval (unit: 10 milliseconds). The value range is 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

Configuring SNMP Flow Control

Command	**snmp-server flow-control pps** *count*
Parameter Description	*count*: Number of SNMP request packets processed per second. The value range is 50 to 65,535.
Command Mode	Global configuration mode
Usage Guide	If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Configuration Example

Setting SNMP Control Parameters

Scenario Figure 1-8	 ● The NMS manages network devices (agents) based on the community authentication mode and can obtain basic system information about the devices, for example, system contact mode, location, and serial number.

Configuration Steps	1. Set SNMP agent parameters. Set the system location, contact mode, and serial number. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	Hostname(config)#snmp-server location fuzhou Hostname(config)#snmp-server contact ruijie.com.cn Hostname(config)#snmp-server chassis-id 1234567890 Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 Hostname(config-if-gigabitEthernet 0/1)#exit
Verification	1. Check the configuration information of the device. 2. Check the SNMP view and group information.
Agent	Hostname# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location fuzhou snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact ruijie.com.cn snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	Hostname#show snmp view v1(include) 1.3.6.1.2.1.1 default(include) 1.3.6.1 Hostname#show snmp group groupname: user1 securityModel: v1 securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview: groupname: user1 securityModel: v2c securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview:

Common Errors

N/A

1.5 Monitoring

Clearing

Description	Command
Clears the list of source IP addresses that are locked after continuous authentication fails.	**clear snmp locked-ip** [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Displaying

Description	Command
Displays the SNMP status.	**show snmp** [**mib** | **user** | **view** | **group** | **host** | **locked-ip** | **process-mib-time**]

1 Configuring RMON

1.1 Overview

The Remote Network Monitoring (RMON) aims at resolving problems of managing local area networks (LANs) and remote sites by using one central point. In RMON, network monitoring data consists of a group of statistics and performance indicators, which can be used for monitoring the network utilization, so as to facilitate network planning, performance optimization, and network error diagnosis.

RMON is mainly used by a managing device to remotely monitor and manage managed devices.

Protocols and Standards

STD 0059 / RFC 2819: Remote Network Monitoring Management Information Base

RFC4502: Remote Network Monitoring Management Information Base Version 2

RFC 3919: Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)

RFC 3737: IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB Modules

RFC 3434: Remote Monitoring MIB Extensions for High Capacity Alarms

RFC 3395: Remote Network Monitoring MIB Protocol Identifier Reference Extensions

RFC 3287: Remote Monitoring MIB Extensions for Differentiated Services

RFC 3273: Remote Network Monitoring Management Information Base for High Capacity Networks

RFC 2896: Remote Network Monitoring MIB Protocol Identifier Macros

RFC 2895: Remote Network Monitoring MIB Protocol Identifier Reference

1.2 Applications

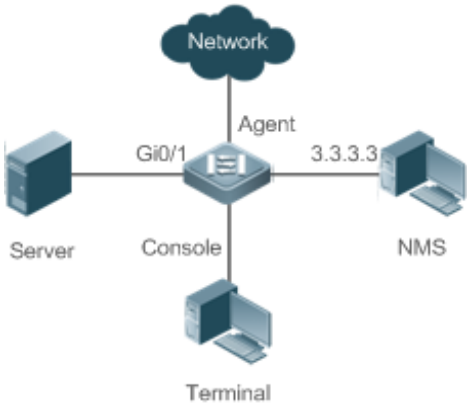
Application	Description
Collecting Statistics on Information of a Monitored Interface	Applies four functions of RMON to an interface to monitor the network communication of the interface.

1.2.1 Collecting Statistics on Information of a Monitored Interface

Scenario

The RMON Ethernet statistics function is used to monitor accumulated information of an interface, the history statistics function is used to monitor the packet count of an interface within each monitoring interval, and the alarm function is used to immediately acquire packet count exceptions of an interface. The following figure shows the networking topology.

Figure 1-1



Deployment

Interface is monitored to accumulatively collect statistics on the packet count of the interface and collect statistics on the packet count and bandwidth utilization of the interface within the monitoring interval. If a packet count exception occurs on the interface, an alarm is reported to the network management system (NMS). The configuration key points are as follows:

- Configure the RMON Ethernet statistics function on interface.
- Configure the RMON history statistics function on interface.
- Configure the RMON alarm table and define RMON event processing actions in configuration mode. Monitored objects of alarms are the object identifier (OID) values of specific fields in the RMON Ethernet statistical table configured for interface.

1.3 Features

Basic Concepts

RMON defines multiple RMON groups. Devices support the statistics group, history group, alarm group, and event group, which are described as follows:

↘ Statistics Group

The statistics group is used to monitor and collect statistics on Ethernet interface traffic information, which is accumulated from the entry creation time to the current time. The statistical items include discarded data packets, broadcast data packets, cyclic redundancy check (CRC) errors, large and small blocks, and collisions. Statistical results are stored in the Ethernet statistical table.

↘ History Group

The history group is used to periodically collect network traffic information. It records accumulated values of network traffic information and the bandwidth utilization within each interval, and saves them in the history control table. It includes two small groups:

- The HistoryControl group is used to set the sampling interval, sampling data source, and other control information.
- The EthernetHistory group provides administrators with historical data, including statistics on network segment traffic, error packets, broadcast packets, utilization, and number of collisions.

Alarm Group

The alarm group is used to monitor a specified Management Information Base (MIB) object. When the value of a MIB object exceeds the preset upper limit or is lower than the preset lower limit, an alarm is triggered and the alarm is processed as an event.

Event Group

The event group is used to define the event processing mode. When a monitored MIB object meets alarm conditions, an event is triggered. An event can be processed in any of the following modes:

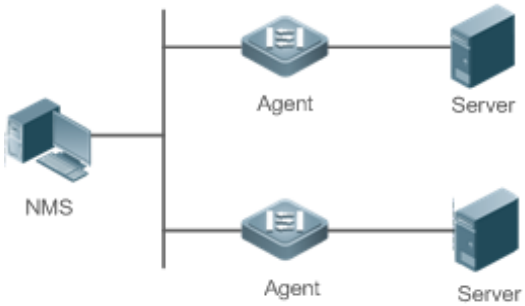
- none: No action is taken.
- log: Event-relevant information is recorded in the log record table so that administrators can view it at any time.
- snmp-trap: A trap message is transmitted to the NMS to notify the NMS of the event occurrence.
- log-and-trap: Event-relevant information is recorded in the log record table and a trap message is transmitted to the NMS.

Working Principle

RMON supports multiple monitors and two data collection methods. Method 1: A dedicated RMON probe is used to collect data and the NMS can directly acquire all information about the RMON MIB from the RMON probe. Method 2: RMON agents are built into network devices (such as switches and routers) so that the devices have the RMON probe function. The NMS uses basic commands of the Simple Network Management Protocol (SNMP) to exchange data with the RMON agents and collect network management information. This method, however, is limited by device resources and information of only four groups rather than all data of the RMON MIB is acquired.

The following figure shows an example of communication between the NMS and RMON agents. The NMS, through the RMON agents running on devices, can acquire information about overall traffic, error statistics, and performance statistics of the network segment where a managed network device interface is, thereby implementing remote management of network devices.

Figure 1-2



Overview

Feature	Description
RMON Ethernet Statistics	Collects statistics on the packet count, byte count, and other data of a monitored Ethernet interface accumulatively.
RMON History Statistics	Records the counts of packets, bytes, and other data communicated by an Ethernet interface within the configured interval and calculates the bandwidth utilization within the interval.

RMON Alarm	Samples values of monitored variables at intervals. The alarm table is used in combination with the event table. When the upper or lower limit is reached, a relevant event table is triggered to perform event processing or no processing is performed.

1.3.1 RMON Ethernet Statistics

Working Principle

The RMON Ethernet statistics function accumulatively collects statistics on network traffic information of an Ethernet interface from the entry creation time to the current time.

Related Configuration

↘ Configuring RMON Statistical Entries

- The RMON Ethernet statistics function is disabled by default.
- Run the **rmon collection stats** command to create Ethernet statistical entries on a specified Ethernet interface.
- After statistical entries are successfully created on a specified interface, the statistics group collects statistics on the traffic information of the current interface. The statistical items are variables defined in the RMON Ethernet statistical table, and recorded information is the accumulated values of variables from the creation time of the RMON statistical table to the current time.

1.3.2 RMON History Statistics

Working Principle

The RMON history statistics function records accumulated statistics on traffic information of an Ethernet interface within each interval.

Related Configuration

↘ Configuring RMON Historical Control Entries

- The RMON history statistics function is disabled by default.
- Run the **rmon collection history** command to create historical control entries on an Ethernet interface.
- The RMON history group collects statistics on variables defined in the RMON history table and records accumulated values of variables within each interval.

1.3.3 RMON Alarm

Working Principle

The RMON alarm function periodically monitors value changes of alarm variables. If the value of an alarm variable reaches the specified upper threshold or lower threshold, a corresponding event is triggered for processing, for example, a trap message is transmitted or one logTable entry record is generated. If a lower threshold or upper threshold is reached

multiple times consecutively, only one corresponding event is triggered and another event is triggered till a reverse threshold is reached.

Related Configuration

Configuring the Event Table

- The RMON event group function is disabled by default.
- Run the **rmon event** command to configure the event table.

Configuring Alarm Entries

- The RMON alarm group function is disabled by default.
- Run the **rmon event** command to configure the event table and run the **rmon alarm** command to configure the RMON alarm table.
- The RMON alarm function is implemented by the alarm table and event table jointly. If a trap message needs to be transmitted to a managing device in the case of an alarm event, the SNMP agent must be correctly configured first. For the configuration of the SNMP agent, see the *Configuring SNMP*.
- If a configured alarm object is a field node in the RMON statistics group or history group, the RMON Ethernet statistics function or RMON history statistics function need to be configured on a monitored Ethernet interface first.

1.4 Configuration

Configuration	Description and Command	
Configuring RMON Ethernet Statistics	(Mandatory) It is used to accumulatively collect statistics on traffic information of an Ethernet interface.	
	rmon collection stats	Configures Ethernet statistical entries.
Configuring RMON History Statistics	(Mandatory) It is used to collect, at intervals, statistics on traffic information of an Ethernet interface and the bandwidth utilization within the interval.	
	rmon collection history	Configures historical control entries.
Configuring RMON Alarm	(Mandatory) It is used to monitor whether data changes of a variable is within the valid range.	
	rmon event	Configures event entries.
	rmon alarm	Configures alarm entries.

1.4.1 Configuring RMON Ethernet Statistics

Configuration Effect

Acquire accumulated statistics on traffic information of a monitored Ethernet interface from the entry creation time to the current time.

Notes

This function cannot be configured in batch interface configuration mode.

Configuration Steps

Configuring RMON Statistical Entries

- Mandatory.
- If statistics and monitoring are required for a specified interface, Ethernet statistical entries must be configured on this interface.

Verification

Run the **show rmon statistics** command to display Ethernet statistics.

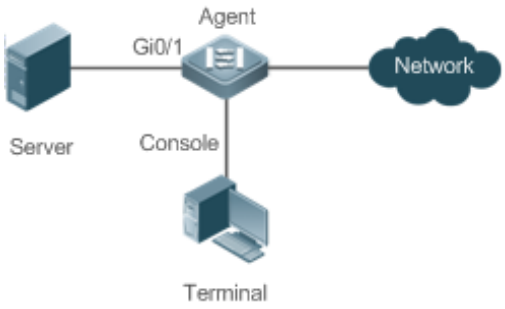
Related Commands

Configuring RMON Statistical Entries

Command	**rmon collection stats** *index* [**owner** *ownername*]
Parameter Description	*index*: Indicates the index number of a statistical entry, with the value ranging from **1** to **65535**. **owner** *ownername*: Indicates the entry creator, which is a case-sensitive string of 1-63 characters.
Command Mode	Interface configuration mode
Usage Guide	The values of statistical entry parameters cannot be changed.

Configuration Example

Configuring RMON Ethernet Statistics

Scenario **Figure 1-3**	
	As shown in the preceding figure, the RMON agent is connected to the server, and the NMS requires the RMON statistics group to conduct performance statistics on received packets of interface Gi0/1. Administrators can view the statistics at any time to understand data about received packets of an interface and take measures in a timely manner to handle network exceptions.
Configuration Steps	● Configure a statistical table instance on interface GigabitEthernet 0/1 to collect statistics on the traffic of this interface.
Agent	Hostname# configure terminal Hostname (config)# interface gigabitEthernet 0/1 Hostname (config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin

Verification	Run the **show rmon stats** command to display Ethernet statistics.
Agent	Hostname# show rmon stats ether statistic table: index = 1 interface = GigabitEthernet 0/1 owner = admin status = 1 dropEvents = 0 octets = 25696 pkts = 293 broadcastPkts = 3 multiPkts = 0 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 packets64Octets = 3815 packets65To127Octets = 1695 packets128To255Octets = 365 packets256To511Octets = 2542 packets512To1023Octets = 152 packets1024To1518Octets = 685

Common Errors

Statistical table entries are re-configured or configured statistical table entries are modified.

1.4.2 Configuring RMON History Statistics

Configuration Effect

Acquire accumulated statistics on the traffic of a monitored Ethernet interface and the bandwidth utilization within each interval.

Notes

This function cannot be configured in batch interface configuration mode.

Configuration Steps

- Mandatory.
- If network statistics on a specified interface need to be collected, RMON historical control entries must be configured on the interface.

Verification

Run the **show rmon history** command to display history group statistics.

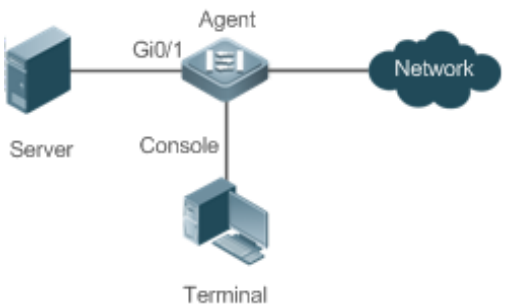
Related Commands

Configuring RMON Historical Control Entries

Command	**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]
Parameter Description	*index*: Indicates the index number of a history statistical entry, with the value ranging from **1** to **65535**. **owner** *ownername*: Indicates the entry creator, which is a case-sensitive string of 1-63 characters. **buckets** *bucket-number*: Sets the capacity of the history table in which a history statistical entry exists. The value ranges from **1** to **65535** and the default value is **10**. **interval** *seconds*: Sets the statistical interval, with the unit of seconds. The value ranges from **1** second to **3600** seconds and the default value is **1800** seconds.
Command Mode	Interface configuration mode
Usage Guide	The values of history statistical entry parameters cannot be changed.

Configuration Example

Configuring RMON History Statistics

Scenario **Figure 1-4**	
	As shown in the preceding figure, the RMON agent is connected to the server, and the NMS needs to collect statistics on received packets of interface Gi0/1 through the RMON history group at an interval of 60 seconds, in an effort to monitor the network and understand emergency data.
Configuration Steps	● Configure the history control table on interface GigabitEthernet 0/1 to periodically collect statistics on the traffic of this interface.
Agent	Hostname# configure terminal Hostname(config)# interface gigabitEthernet 0/1

	Hostname(config-if-GigabitEthernet 0/1)# rmon collection history 1 buckets 5 interval 300 owner admin
Verification	Run the **show rmon history** command to display history group statistics.
Agent	Hostname# show rmon history rmon history control table: index = 1 interface = GigabitEthernet 0/1 bucketsRequested = 5 bucketsGranted = 5 interval = 60 owner = admin stats = 1 rmon history table: index = 1 sampleIndex = 786 intervalStart = 6d:18h:37m:38s dropEvents = 0 octets = 2040 pkts = 13 broadcastPkts = 0 multiPkts = 0 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 utilization = 0 index = 1 sampleIndex = 787 intervalStart = 6d:18h:38m:38s

dropEvents = 0

octets = 1791

pkts = 16

broadcastPkts = 1

multiPkts = 0

crcAlignErrors = 0

underSizePkts = 0

overSizePkts = 0

fragments = 0

jabbers = 0

collisions = 0

utilization = 0

index = 1

sampleIndex = 788

intervalStart = 6d:18h:39m:38s

dropEvents = 0

octets = 432

pkts = 6

broadcastPkts = 0

multiPkts = 0

crcAlignErrors = 0

underSizePkts = 0

overSizePkts = 0

fragments = 0

jabbers = 0

collisions = 0

utilization = 0

index = 1

sampleIndex = 789

intervalStart = 6d:18h:40m:38s

dropEvents = 0

octets = 432

```
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 790
intervalStart = 6d:18h:41m:38s
dropEvents = 0
octets = 86734
pkts = 934
broadcastPkts = 32
multiPkts = 23
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0
```

Common Errors

History control table entries are re-configured or configured history control table entries are modified.

1.4.3 Configuring RMON Alarm

Configuration Effect

Periodically monitor whether value changes of alarm variables are within the specified valid range.

Notes

If a trap message needs to be transmitted to a managing device when an alarm event is triggered, the SNMP agent must be correctly configured. For the configuration of the SNMP agent, see the *Configuring SNMP*.

If an alarm variable is a MIB variable defined in the RMON statistics group or history group, the RMON Ethernet statistics function or RMON history statistics function must be configured on the monitored Ethernet interface. Otherwise, an alarm table fails to be created.

Configuration Steps

Configuring Event Entries

- Mandatory.
- Complete the configuration in global configuration mode.

Configuring Alarm Entries

- Mandatory.
- Complete the configuration in global configuration mode.

Verification

- Run the **show rmon event** command to display the event table.
- Run the **show rmon alarm** command to display the alarm table.

Related Commands

Configuring the Event Table

Command	**rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]
Parameter Description	*number*: Indicates the index number of an event table, with the value ranging from **1** to **65535**. **log**: Indicates a log event. The system logs a triggered event. **trap** *community*: Indicates a trap event. When an event is triggered, the system transmits a trap message with the community name of *community*. **description** *description-string*: Sets the description information about an event. The value is a string of 1-127 characters. **owner** *ownername*: Indicates the entry creator, which is a case-sensitive string of 1-63 characters.
Command Mode	Global configuration mode
Usage Guide	The values of configured event entry parameters can be changed, including the event type, trap community name, event description, and event creator.

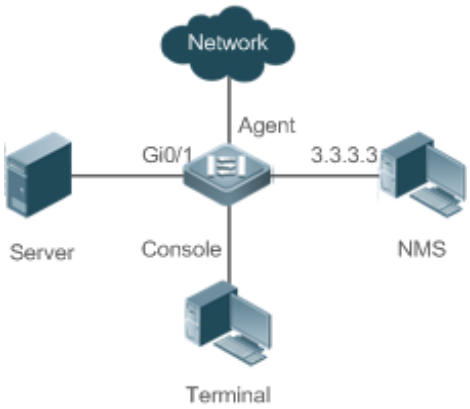
Configuring the RMON Alarm Group

Command	**rmon alarm** *number variable interval* {**absolute	delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]
Parameter Description	*number*: Indicates the index number of an alarm entry, with the value ranging from **1** to **65535**. *variable*: Indicates an alarm variable, which is a string of 1-255 characters and is represented in dotted format using the node OID (format: entry.integer.instance; example: 1.3.6.1.2.1.2.1.10.1). *interval*: Indicates the sampling interval, with the unit of seconds and the value ranging from **1** to **2147483647**.

	absolute: Indicates that the sampling type is absolute value sampling, that is, variable values are directly extracted when the sampling time is up. **delta**: Indicates that the sampling type is changing value sampling, that is, changes in the variable values within the sampling interval are extracted when the sampling time is up. **rising-threshold** *value*: Sets the upper limit of the sampling quantity (*value*), with the value ranging from **-2147483648** to **+2147483647**. *event-number:* Indicates that an event with the event number of *event-number* is triggered when the upper limit or lower limit is reached. **falling-threshold** *value*: Sets the lower limit of the sampling quantity (*value*), with the value ranging from **-2147483648** to **+2147483647**. **owner** *ownername*: Indicates the entry creator, which is a case-sensitive string of 1-63 characters.
Command Mode	Global configuration mode
Usage Guide	Values of configured alarm entry parameters can be changed, including alarm variables, sampling type, entry creator, sampling interval, upper/lower limit of the sampling quantity, and relevant trigger events.

Configuration Example

Configuring RMON Alarm

Scenario **Figure 1-5**	
	Assume that SNMPv1 runs on the NMS, the community name used for accessing the settings is public, with the attribute of read-write, and the IP address used by the NMS to receive trap messages is 3.3.3.3. Assume that the OID value of unknown protocol packets received by monitored interface GigabitEthernet0/1 is 1.3.6.1.2.1.2.2.1.15.3, the sampling mode is relative sampling, and the sampling interval is 60 seconds. When the relative sampling value is larger than 100 or lower than 10, event 1 and event 2 are triggered respectively. In event 1, a trap message is transmitted and the event is logged. In event 2, the event is only logged. The configuration of the RMON agent is completed on the terminal. The RMON agent is connected to the NMS and is connected to the server through interface Gi0/1. The RMON agent needs to monitor the count of unknown protocol packets received by interface Gi0/1. The sampling interval is 60 seconds. When the absolute sampling value is smaller than 10, the event is only logged. When the absolute sampling value is larger than 100, the event is logged and a trap message is transmitted to the NMS.

Configuration Steps	● Configure the host address for receiving trap messages. ● Configure an event group to process alarm trigger. ● Configure the alarm function.
Agent	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# snmp-server community public rw Hostname(config)# snmp-server host 3.3.3.3 trap public Hostname(config)# rmon event 1 description rising-threshold-event log trap public owner admin Hostname(config)# rmon event 2 description falling-threshold-event log owner admin Hostname(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1 falling-threshold 10 2 owner admin
Verification	● Run the **show rmon event** command to display the event table. ● Run the **show rmon alarm** command to display the alarm table.
Agent	Hostname# show rmon event rmon event table: index = 1 description = rising-threshold-event type = 4 community = public lastTimeSent = 0d:0h:0m:0s owner = admin status = 1 index = 2 description = falling-threshold-event type = 2 community = lastTimeSent = 6d:19h:21m:48s owner = admin status = 1 rmon log table: eventIndex = 2 index = 1

```
                    logTime = 6d:19h:21m:48s
                    logDescription = falling-threshold-event
Hostname# show rmon alarm
rmon alarm table:
        index: 1,
        interval: 60,
        oid = 1.3.6.1.2.1.2.2.1.15.3
        sampleType: 2,
        alarmValue: 0,
        startupAlarm: 3,
        risingThreshold: 100,
        fallingThreshold: 10,
        risingEventIndex: 1,
        fallingEventIndex: 2,
        owner: admin,
        stauts: 1
```

Common Errors

- The entered OID of a monitored object is incorrect, the variable corresponding to the OID does not exist, or the type is not an integer or unsigned integer.
- The upper threshold is smaller than or equal to the lower threshold.

1.5 Monitoring

Displaying

Description	Command
Displays all RMON configuration information.	**show rmon**
Displays the Ethernet statistical table.	**show rmon statistics**
Displays the history control table.	**show rmon history**
Displays the alarm table.	**show rmon alarm**
Displays the event table.	**show rmon event**

1 Configuring CWMP

1.1 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

1.2 Applications

N/A

1.3 Features

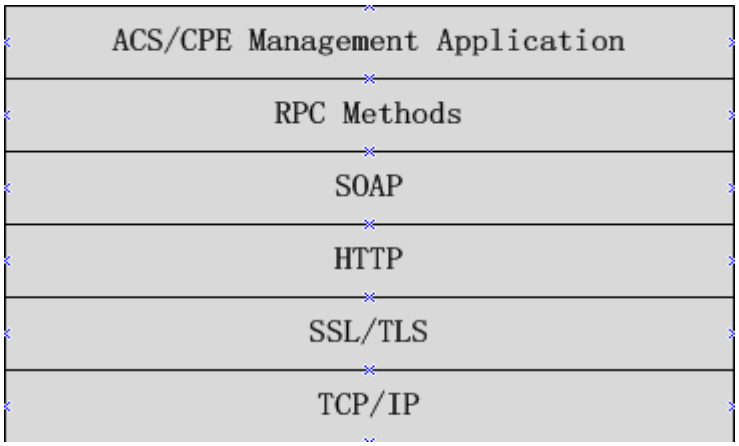
Basic Concept

Major Terminologies

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

Protocol Stack

Figure 1-1 CWMP Protocol Stack



As shown in Figure 1-1, 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.

DM nodes can also be classified into readable nodes and readable-and-writable nodes. A readable node is a node whose parameter values can be read but cannot be modified, and a readable-and-writable node is a node whose parameter values can be both read and modified.

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.

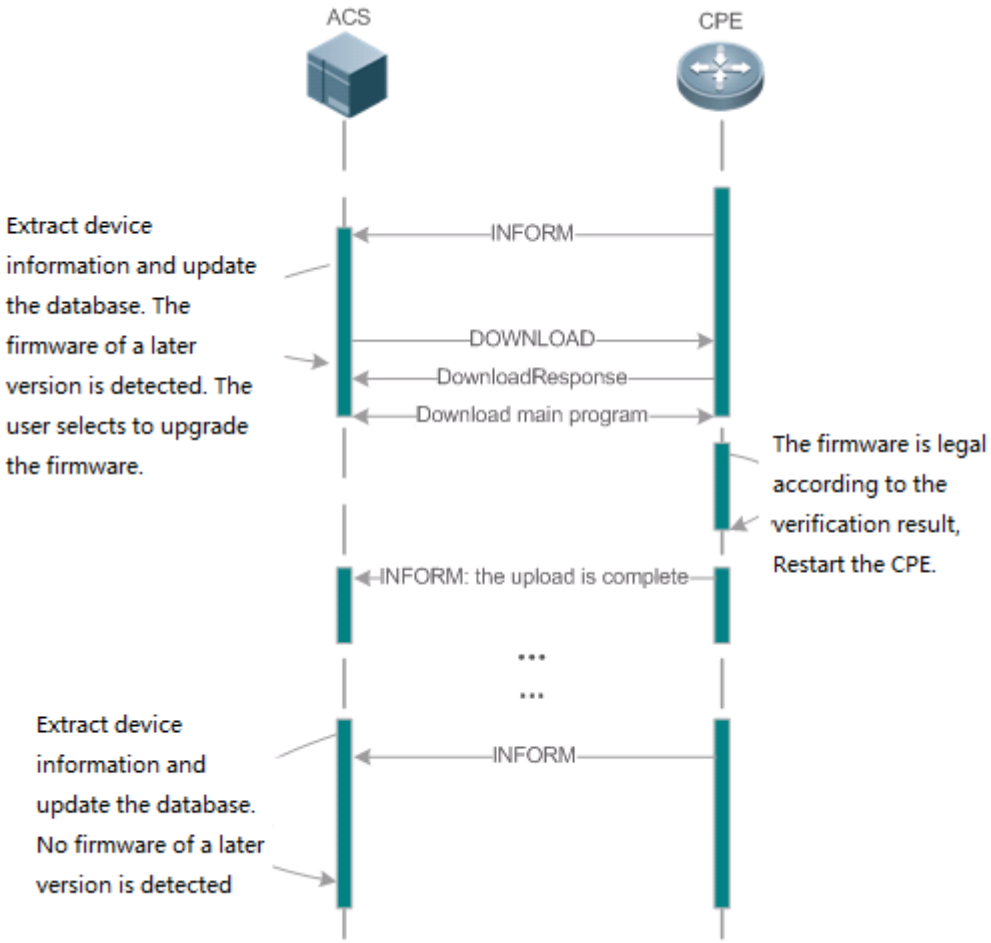
1.3.1 Upgrading the Firmware

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 1-2



Users specify a CPE for the ACS to deliver the Download method for upgrading the firmware. The CPE receives the request and starts to download the latest firmware from the destination file server, upgrade the firmware, and then reboot. After restart, the CPE will indicate the successful or unsuccessful completion of the method application.

The file server can be ACS or separately deployed.

Related Configuration

Enabling CWMP

- CWMP is enabled by default.
- Run the **cwmp** command to enable CWMP in global configuration mode.

Configuring the ACS URL

- No ACS URL is configured by default.
- Run the **acs url** command to configure the ACS URL in CWMP configuration mode.

Configuring the ACS Username for CWMP Connection

- No ACS username is configured for CWMP connection by default.
- Run the **acs usrname** command to configure the ACS username for CWMP connection in CWMP configuration mode.

Configuring the ACS Password for CWMP Connection

- No ACS password is configured for CWMP connection by default.
- Run the **acs password** command to configure the ACS password for CWMP connection in CWMP configuration mode.

Configuring the CPE URL

- No CPE URL is configured by default.
- Run the **cpe url** command to configure the CPE URL in CWMP configuration mode.

Configuring the CPE Username for CWMP Connection

- No CPE username is configured for CWMP connection by default.
- Run the **cpe usrname** command to configure the CPE username for CWMP connection in CWMP configuration mode.

Configuring the CPE Password for CWMP Connection

- No CPE password is configured for CWMP connection by default.
- Run the **cpe password** command to configure the CPE password for CWMP connection in CWMP configuration mode.

Enabling the Periodic Notification Function for the CPE

- The CPE notification interval is 600s by default.
- Run the **cpe inform** command to configure the periodic notification function for the CPE in CWMP configuration mode.

Configuring the ACS Response Timeout for the CPE

- The ACS response timeout for the CPE is 30s by default.
- Run the **timer cpe-timeout** command to configure the ACS response timeout for the CPE in CWMP configuration mode.

Configuring the CPE to Download Files

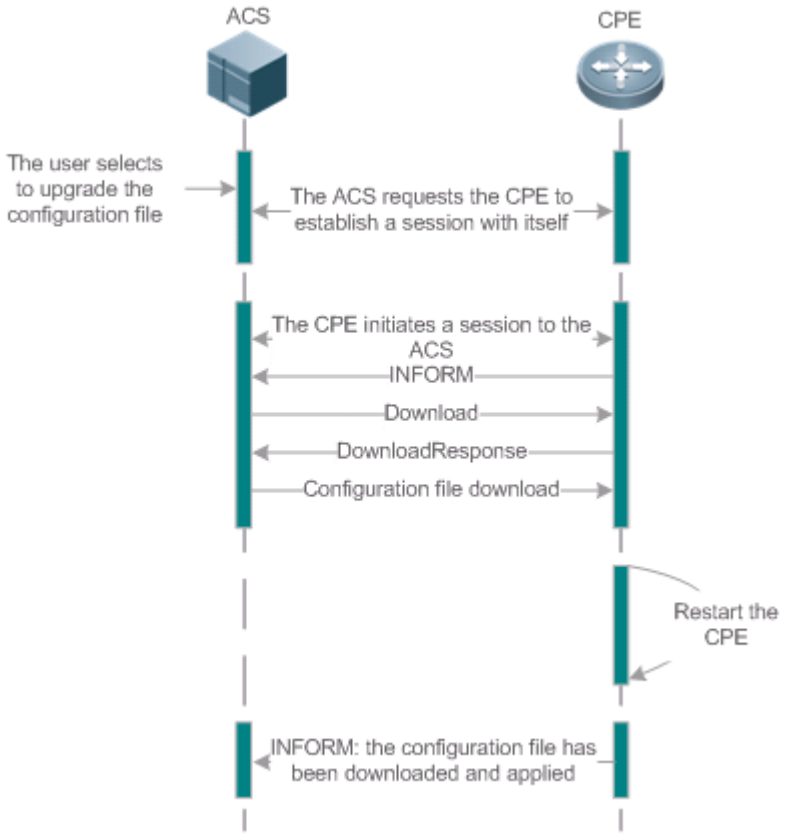
- The function is enabled by default.
- Run the **no disable download** command to enable the CPE to download firmware and configuration files from the ACS.

1.3.2 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 1-3



Users specify a CPE for the ACS to deliver the Download methods for upgrading its configuration files. The CPE downloads the configuration files from the specified file server, upgrade configuration files, and then reboot. After that, the CPE will indicate successful or unsuccessful completion of the method application.

The file server can be ACS or separately deployed.

Related Configuration

Enabling CWMP

The configuration is the same as that in Upgrading the Firmware.

Configuring the ACS URL

The configuration is the same as that in in Upgrading the Firmware.

Configuring the ACS Username for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Configuring the ACS Password for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE URL

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE Username for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE Password for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Enabling the Periodic Notification Function for the CPE

The configuration is the same as that in in Upgrading the Firmware.

Configuring the ACS Response Timeout for the CPE

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE to Download Files

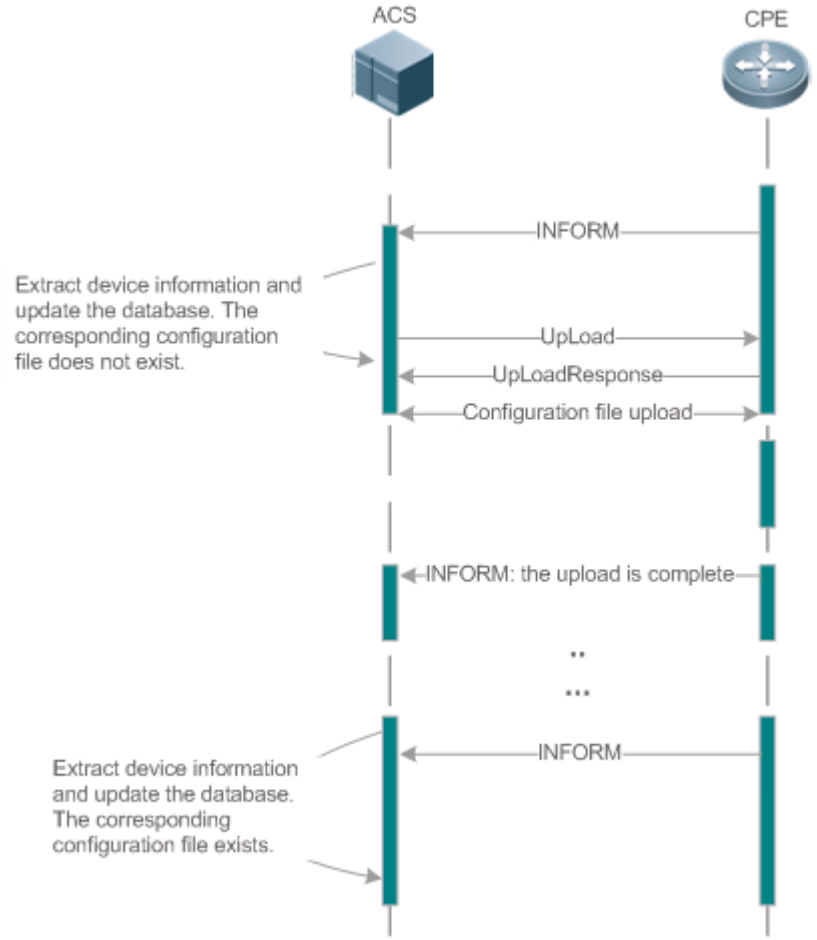
The configuration is the same as that in in Upgrading the Firmware.

1.3.3 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 1-4



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.

Related Configuration

↘ Enabling CWMP

The configuration is the same as that in in Upgrading the Firmware.

↘ Configuring the ACS URL

The configuration is the same as that in in Upgrading the Firmware.

Configuring the ACS Username for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Configuring the ACS Password for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE URL

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE Username for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE Password for CWMP Connection

The configuration is the same as that in in Upgrading the Firmware.

Enabling the Periodic Notification Function for the CPE

The configuration is the same as that in in Upgrading the Firmware.

Configuring the ACS Response Timeout for the CPE

The configuration is the same as that in in Upgrading the Firmware.

Configuring the CPE to Upload and Download Files

- The function is enabled by default.
- Run the **no disable upload** command to enable the CPE to download configuration files delivered from the ACS and upload log files to the ACS.

1.3.4 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.

Related Configuration

Configuring CPE Backup and Restoration

- The function is enabled by default. The default restoration time is 60 seconds.
- Run the **cpe back-up** command to configure the backup and restoration of the firmware and configuration file of the CPE.
- A larger restoration time value indicates a longer restoration delay.

1.4 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 for the CPE.
	cpe back-up	Configures the backup and restoration of the firmware and configuration file of the CPE.
	disable download	Disables the management function of main program and configuration files delivered and downloaded by the ACS.

Action	Suggestions and Related Commands	
	disable stun	Disables STUN port adaptation and NAT timeout detection.
	disable upload	Disables the management function of uploading configuration and log files to the ACS.
	stun max-period	Configures the maximum STUN keepalive interval.
	stun min-period	Configures the minimum STUN keepalive interval.
	stun port	Configures the STUN server port.
	timer cpe- timeout	Configures the ACS response timeout on CPEs.

1.4.1 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

- The CWMP function is enabled by default.
- Mandatory.
- Configure this function on the CPE.

Command	cwmp
Parameter Description	N/A
Defaults	CWMP is enabled by default.
Command Mode	Global configuration guide

Usage Guide	N/A

Configuring the ACS Username for CWMP Connection

- This configuration is mandatory on the ACS.
- Only one username can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs username** *username*
Parameter Description	**username** *username*: The ACS username for CWMP connection
Defaults	The ACS username is not configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Password for CWMP Connection

- This configuration is mandatory on the ACS.
- The password of the ACS can be in cleartext or encrypted form. Only one password can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs password** {*password* | *encryption-password encrypted-password*}
Parameter Description	*password:* ACS password *encryption-password:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-password*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Username for CWMP Connection

- This configuration is mandatory on the CPE.
- Only one username can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe username** *username*
Parameter Description	*username*: CPE username
Defaults	No CPE username is configured by default.

Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Password for CWMP Connection

- This configuration is mandatory on the CPE.
- The password of the CPE can be in cleartext or encrypted form. Only one password can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe password** {*password* | *encryption-password encrypted-password*}
Parameter Description	*password:* CPE password *encryption-password:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-password*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements: ● Contain 1 to 26 characters including letters and figures. ● The leading spaces will be ignored, while the trailing and middle are valid.

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 Description	*url*: ACS URL
Defaults	No ACS URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If the ACS URL is not configured but obtained through DHCP, CPEs will use this dynamic URL to initiate connection to the ACS. The ACS URL must: ● Be in format of **http://ip [: port]/ path**. ● Contain 255 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 Description	*url:* CPE URL
Defaults	No CPE URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If CPE URL is not configured, it is obtained through DHCP. The CPE URL must: ● Be in format of **http://ip [: port]/**. ● Contain 255 characters at most.

Configuration Examples

The following configuration examples describe CWMP-related configuration only.

Configuring Usernames and Passwords on the CPE

Network Environment **Figure 1-5**	
Configuration Method	● Enable CWMP. ● On the CPE, configure the ACS username and password to be authenticated for the CPE to connect to the ACS. ● On the CPE, configure the CPE username and password to be authenticated for the ACS to connect to the CPE.
CPE	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# cwmp Hostname(config-cwmp)# acs password PASSWORDB Hostname(config-cwmp)# cpe username USERB Hostname(config-cwmp)# cpe password PASSWORDB
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname # show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : USERB

	CPE password : ******

Configuring the URLs of the ACS and the CPE

Network Environment	See **Figure 1-5**.
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.
CPE	Hostname# configure terminal Hostname(config)# cwmp Hostname(config-cwmp)# cpe url http://10.10.10.1:7547/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/

Common Errors

- If the entered password is in cyphertext and it is not an even number or its length is less than 2 characters or not more than 254 characters, the following prompt will be displayed:
- The user-input cleartext password is longer than 126 characters.
- The user-input cleartext password contains illegal characters.
- The URL of the ACS is set to **NULL**.
- The URL of the CPE is set to **NULL**.

1.4.2 Configuring CWMP-Related Attributes

Configuration Effect

- You can configure common functions for CPE, for example, backup and restoration of main program and configuration files, acceptance or not of main program and configuration files delivered by the ACS , management or not of configuration/log files uploaded to the ACS.

Configuration Method

Configuring the Periodic Notification Function for the CPE

- (Optional) The value range is from 30 to 3,600 in seconds. The default value is 300 seconds.
- Perform this configuration to reset the periodical notification interval for the CPE.

Command	**cpe inform** [**interval** *seconds*] [**start-time** *time*]
Parameter Description	*seconds*: Specifies the periodical notification interval for the CPE in seconds. The value ranges from 30 to 3,600. *time*: Specifies the date and time for starting periodical notification in *yyyy-mm-ddThh:mm:ss* format.
Command Mode	CWMP configuration mode
Defaults	The default value is 300 seconds.
Usage Guide	Use this command to configure the periodic notification function for the CPE. ● If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval. ● If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

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

- (Optional) The CPE can download firmware and configuration files from the ACS by default.
- Perform this configuration if the CPE does not need to download firmware and configuration files from the ACS.

Command	**disable download**
Parameter Description	N/A
Defaults	The CPE can download firmware and configuration files from the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of downloading main program and configuration files from the ACS. ● This command does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.

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

- (Optional.) The CPE can upload configuration and log files to the ACS by default.
- Perform this configuration if the CPE does not need to upload configuration and log files to the ACS.

Command	**disable upload**
Parameter Description	N/A

Defaults	The CPE can upload configuration and log files to the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

Disabling STUN Port Adaptation and NAT Timeout Detection

- (Optional) Use this command to disable STUN port adaptation and NAT **t**imeout **d**etection.
- STUN port adaptation and NAT timeout detection are disabled by default.

Command	**disable stun** { **port-adaptive** | **probe-agingtime** }
Parameter Description	**port-adaptive**: Configures STUN port adaptation. **probe-agingtime**: Configures NAT timeout detection.
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	*seconds*: Specifies the delay for backup and restoration of the firmware and configuration file of the CPE.
Defaults	The default value is 60 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the Maximum STUN Keepalive Interval

- (Optional) Use this command to configure the maximum STUN keepalive interval.
- The default maximum STUN keepalive interval is 60 seconds.

Command	**stun max-period** *interval*
Parameter Description	*interval*: Configures the maximum STUN keepalive interval in seconds. The value range is from 0 to 3600. The default value is 60.

Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the Minimum STUN Keepalive Interval

- (Optional) Use this command to configure the minimum STUN keeaplive interval.
- The default minimum STUN keepalive interval is 20 seconds.

Command	**stun min-period** *interval*
Parameter Description	*interval*: Configures the minimum STUN keepalive interval in seconds. The value range is from 0 to 3600. The default value is 20.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the STUN Server Port

- (Optional) Use this command to configure the STUN server port.
- The default STUN server port is 3478.

Command	**stun port** *port-number*
Parameter Description	*port-number*: Configures the STUN server port. The value range is from 0 to 65535. The default value is 3478.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Response Timeout

- (Optional) The value range is from 10 to 600 in seconds. The default value is 30 seconds.
- Perform this configuration to modify the ACS response timeout period on the CPE.

Command	**timer cpe-timeout** *seconds*
Parameter Description	*seconds*: Specifies the timeout period in seconds. The value range is from 10 to 600.
Defaults	The default value is 30 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Verification

- Run the **show cwmp configuration** command.

Command	show cwmp configuration
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	The following example displays the CWMP configuration. Hostname(config-cwmp)#show cwmp configuration CWMP Status : enable ACS URL : http://www.ruijie.com.cn/acs ACS username : admin ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : 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

Configuration Examples

Configuring the Periodical Notification Interval for the CPE

Network Environment	See **Figure 1-5**.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval for the CPE to 60 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)#cpe inform interval 60
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie #show cwmp configuration

Network Environment	See **Figure 1-5**.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval for the CPE to 60 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)#cpe inform interval 60
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
	CWMP Status : enable ..... CPE inform interval : 60s

Disabling the Management Function of Main Program and Configuration Files Delivered and Downloaded by the ACS

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the management function of main program and configuration files delivered and downloaded by the ACS.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)#disable download
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE download status : disable

Disabling STUN Port Adaptation and NAT Timeout Detection

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable STUN port adaptation. ● Disable NAT timeout detection.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)#disable stun port-adaptive Hostname(config-cwmp)#disable stun probe-agingtime
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE STUN port-adaptive : disable CPE STUN probe nat agingtime : disable

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

Network Environment	See **Figure 1-5**.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the management function of uploading configuration and log files to the ACS.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# disable upload
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE upload status : disable

Configuring the Backup and Restoration Delay

Network Environment	See **Figure 1-5**.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 100 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# cpe back-up Seconds 30
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE back up delay time : 30s

Configuring the Maximum STUN Keepalive Interval

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the maximum STUN keepalive interval to 1000 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# stun max-period 1000
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable ..... CPE STUN max-period : 1000s

Configuring the Minimum STUN Keepalive Interval

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the minimum STUN keepalive interval to 100 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# stun min-period 100
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the minimum STUN keepalive interval to 100 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# stun min-period 100
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
	…… CPE STUN max-period : 100s

Configuring the STUN Server Port

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the STUN server port to 4000.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# stun port 4000
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable …… CPE STUN port : 4000

Configuring the Backup and Restoration Delay

Network Environment	See **Figure 1-5**.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 30 seconds.
CPE	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#cwmp Hostname(config-cwmp)# cpe back-up Seconds 30
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname #show cwmp configuration CWMP Status : enable …… CPE back up delay time : 30s

↘ Configuring the ACS Response Timeout of the CPE

Network Environment	See **Figure 1-5**.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the response timeout of the CPE to 100 seconds.
CPE	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# cwmp Hostname(config-cwmp)# timer cpe-timeout 100
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Hostname#show cwmp configuration CWMP Status : enable ..... CPE wait timeout : 100s

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays the CWMP configuration.	**show cwmp configuration**
Displays the CWMP running status.	**show cwmp status**

1 Configuring RPCAP

Whether this function is supported depends on the product version.

1.1 Overview

Remote Packet Capture Protocol (RPCAP) is a protocol used for remote wireless sniffing. Remote packet capture enables users to collect wireless fault information conveniently and promptly, troubleshoot wireless client faults in time, and improve wireless network quality.

The remote packet capture function captures wireless packets sent and received on the radio port of an access point (AP) by accessing and controlling the AP through a remote host. This function, making full use of the AP deployed in the wireless network, can realize wireless data capture on the entire network and remotely analyze the captured wireless data in real time.

Remote packet capture works in a listening mode, dedicated to sniff wireless packets within its signal coverage scope. When packets are being captured in the listening mode, connection status and packet interaction of users associated with the corresponding RF port cannot be guaranteed.

Protocols and Standards

N/A

1.2 Applications

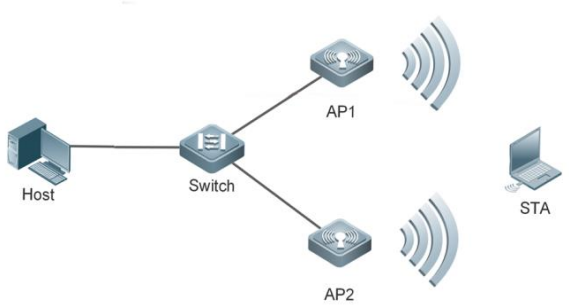
Application	Description
Remote packet capture in fat AP mode	In fat AP mode, enable the wireless sniffing service on the AP. The remote host sniffs packets on the radio port of the AP through packet sniffing tools.

1.2.1 Remote Packet Capture in Fat AP Mode

Scenario

In Fat AP mode, the remote host enables the monitoring mode on the radio 2 port of the AP 1 through packet sniffing tools that support RPCAP and captures wireless packets (including packets between the STA and the radio 2 port of the AP 2 which shares the same channel with the radio 2 port of the AP 1), as shown in the following figure.

Figure 1-1 RPCAP Remote Packet Capture in Fat AP Mode



Deployment

- Configure the radio 2 port as the port for packet capture on the AP 1.
- Use Wireshark on the remote host to sniff packets.

1.3 Features

Basic Concepts

STA, AP and AC

STA: Indicates wireless station with wireless network interface cards (NICs), for example, a laptop or a mobile phone.

AP: Indicates the wireless access point that provides wireless signals for STAs to access the network.

AC: Indicates the wireless controller that provides wireless connection and related services.

Control Channel and Data Channel

RPCAP uses the control channel and data channel to communicate with the packet sniffing tool.

Control channel: Transmits signaling based on reliable TCP connection.

Data channel: Transmits captured data based on TCP or UDP.

Features

Feature	**Description**
Remote packet capture function	Indicates that a remote host accesses an AP and captures packets sent and received on the radio port of the AP.

1.3.1 Remote Packet Capture Function

The remote packet capture function allows a remote host to access an AP and capture packets sent and received on the radio port of the AP. This function realizes wireless data sniffing on the entire network and remotely analyzes the sniffed wireless data in real time.

Working Principle

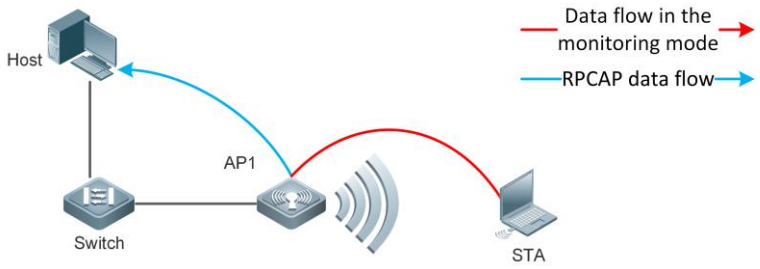
The remote packet capture function is based on the RPCAP protocol. RPCAP uses the control channel and data channel to communicate with the packet sniffing tool. The control channel is used to transmit signaling based on reliable TCP connection. The data channel is used to transmit captured data based on TCP or UDP. The RPCAP protocol defines a total of 18 control message types, including authentication, interface retrieval, sampling rate, filter rules, statistics handling, and control for initiating, stopping, and terminating sniffing operations. Additionally, it defines a data message type dedicated for identifying sniffed data packets.

The working principle of remote packet capture involves implementing the RPCAP protocol on Ruijie APs. This enables remote hosts to control the wireless sniffing process on the radio port of APs and analyze the wireless data in real time using RPCAP-supporting sniffing tools. The following figure shows the data flow and working process of remote packet capture:

The remote host accesses, controls, and enables the wireless sniffing function on the radio port of the AP.

1. The radio port of the AP begins wireless sniffing.
2. The AP adds antenna information to the captured wireless packets and encapsulates them with the RPCAP protocol header before sending them to the remote host.
3. The remote host uses a tool that supports RPCAP (such as Wireshark) to analyze and process the packets.

Figure 1-2 Remote Packet Capture Data Flow



Note: Switch: Indicates a switch.
Host: Indicates a remote host.

1.4 Configuration

Configuration	Description and Command

Configuring Wireless Sniffing	(Mandatory) It is used to configure the wireless sniffing function on a specified AP radio port.	
	wlan-cap enable	Configures the wireless sniffing function on a radio port.
Configuring RPCAP Remote Access Information	(Optional) It is used to configure the listening TCP port accessed remotely by RPCAP and login information for remote host access.	
	rpcap port	Configures the listening TCP port number.
	rpcap login	Configures login information for remote host access.
	wlan-cap	Creates or enters the sniffing configuration mode.
Enabling the Wireless Sniffing Service	(Mandatory) It is used to enable or disable the wireless sniffing service.	
	wlan-cap	Enters the wireless sniffing mode.
	service enable	Enables/Disables the wireless sniffing service.

1.4.1 Configuring the Wireless Sniffing Function

Configuration Effect

Enable the wireless sniffing function on the specified RF port of the fat AP to obtain wireless packets within the sniffing signal coverage scope, including communication packets between the AP and the STA.

Notes

N/A

Configuration Steps

↘ Configuring the Wireless Sniffing Function

- Mandatory.
- To implement remote wireless sniffing on a specified port, add the port into the sniffing port list on the AP.
- Use the **wlan-cap enable radio** *radio-id* command to enable the wireless sniffing function on this port.
- When the radio port of the AP is added into the wireless sniffing port list, the wireless sniffing function will be enabled on this port.

Command	**wlan-cap enable** { **radio** *radio-id* | **eth** *eth-id* }
Parameter Description	*radio-id*: Indicates the RF port ID. *eth-id*: Indicates the Ethernet port ID.

Defaults	The wireless sniffing function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The wireless sniffing function can be enabled only on the RF port of the online AP that supports wireless sniffing.

Verification

Run the **show wlan-cap interface** command to check whether the wireless sniffing function is enabled.

Configuration Example

↘ Enabling Wireless Sniffing on the Specified RF Port of the AP in Fat AP Mode

Configuration Steps	Use this command to enable the wireless sniffing function on the radio 1 port of the AP.
AP	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# wlan-cap Hostname(wlan-cap)# enable radio 1
Verification	Run the following command to display wireless sniffing configuration on a specified port.
AP	Hostname(wlan-cap)#show wlan-cap interface Total Interface : 1 Total capturing Interface : 0 Total Idle Interface : 1 AP Name MAC Address Type Index Channel Status Users ---------- ---------- ----- ----- ------- ------- ----- AP180-SF 00d0.f019.9324 radio 1 1 Idle 0

Common Error

N/A

1.4.2 Configuring RPCAP Remote Access Information

Configuration Effect

- Configuring RPCAP remote access information includes configuring the listening TCP port for RPCAP remote access and login information for remote host access
- The listening TCP port for RPCAP remote access is port 2002 by default.

Notes

- The wireless sniffing configuration mode must be entered first.

- The listening port can be configured only when wireless sniffing is disabled. The configured TCP port must be a currently idle port. (Use the **show tcp port** command to check the status of TCP ports.) Otherwise, a port binding failure may occur when wireless sniffing is enabled (the console will display related information).
- Login information can be configured only when wireless sniffing is disabled. The maximum length of both the username and the password is 64 characters.

Configuration Steps

Entering the Wireless Sniffing Configuration Mode

- Optional.
- The listening port and login information can be configured only on the fat AP.

Command	**wlan-cap**
Parameter Description	N/A
Defaults	The wireless sniffing configuration mode is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Listening Port

- Optional.
- The listening port can be configured only on the fat AP.

Command	**rpcap port** *port-value*
Parameter Description	**port-value**: Indicates the listening port number. The value ranges from 1 to 65535.
Defaults	The default value is 2002.
Command Mode	Wireless sniffing configuration mode
Usage Guide	N/A

Configuring Login Information

- Optional.
- Login information for remote host access can be configured only on the fat AP.
- Configuring RPCAP remote access information includes configuring the port to be accessed and the username and password used for remote host login.

Command	**rpcap login** *username password*
Parameter Description	*username*: Indicates the username used for login. *password*: Indicates the password used for login.
Defaults	No username and password are configured by default.

Command Mode	Wireless sniffing configuration mode
Usage Guide	N/A

Verification

Run the **show wlan-cap config** command to display wireless sniffing configuration.

Configuration Example

Setting the Listening Port Number of the Fat AP to 65535 in Fat AP Mode

Scenario **Figure** 1-3	
Configuration Steps	● Use this command to enter the wireless sniffing configuration mode and set the listening port to 65535 for RPCAP remote access.
Fat AP	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#wlan-cap Ruijie(wlan-cap)#rpcap port 65535
Verification	Run the following command to display wireless sniffing configuration.
Fat AP	Ruijie#show wlan-cap config ========================== Wlan-cap-config ====================== Listen port: 65535 Login info: Anonymous Forward: Central Service enable: No

Configuring Login Information for the Fat AP

Configuration Steps	● Use this command to enter the wireless sniffing configuration mode and set the username and password for RPCAP remote access to **wlan-capture**.
Fat AP	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#wlan-cap Ruijie(wlan-cap)#rpcap login wlan-capture wlan-capture
Verification	Run the following command to display wireless sniffing configuration.

Fat AP	Ruijie#show wlan-cap config ========== Wlan-cap-config ========== Listen port: 2002 Login info: wlan-capture : wlan-capture Forward: Central Service enable: No

Common Error

N/A

1.4.3 Enabling Wireless Sniffing

Configuration Effect

The wireless sniffing service can be used normally only after the wireless sniffing function is enabled.

Notes

After wireless sniffing is enabled, only the sniffed channel can be modified, and the other configurations cannot be modified in this configuration mode.

Configuration Steps

↘ Configuring Wireless Sniffing

- Mandatory.
- To use the wireless sniffing function on the fat AP, you must enable this service first.
- Use the **service enable** command to enable wireless sniffing.

Command	**service enable**
Parameter Description	N/A
Defaults	Wireless sniffing is disabled by default.
Command Mode	Wireless sniffing configuration mode
Usage Guide	After wireless sniffing is enabled, only the sniffed channel can be modified, and the other configurations cannot be modified in this configuration mode.

Verification

Run the **show wlan-cap config** command to check whether wireless sniffing is enabled.

Configuration Example

↘ Configuring Wireless Sniffing on the Fat AP

Scenario **Figure** 1-4	
Configuration Steps	● Use this command to enter the wireless sniffing configuration mode and enable wireless sniffing on the fat AP.
Fat AP	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# wlan-cap Ruijie(wlan-cap)# service enable
Verification	Run the following command to display wireless sniffing configuration on the fat AP.
Fat AP	Ruijie#show wlan-cap config ========================== Wlan-cap-config ====================== Listen port: 2002 Login info: Anonymous Forward: Central Service enable: Yes

Common Error

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Function
show wlan-cap config	Displays wireless sniffing configuration.
show wlan-cap state	Displays current sniffing status.
show wlan-cap interface	Displays sniffing interface information.

Debugging

N/A

Configuring VPN

1. Configuring Ipsec
2. Configuring PPPoE Client

1 Configuring IPsec

1.1 Overview

IP Security (IPsec) is a Layer-3 tunnel encryption protocol formulated by the Internet Engineering Task Force (IETF). It provides high-quality, interoperable, and cryptology-based security guarantee for data transmitted in the Internet. IPsec provides the following security services for specific communication parities at the IP layer via encryption and data authentication:

- Confidentiality: The IPsec sender encrypts packets prior to packet transmission in a network.
- Data integrity: The IPsec receiver authenticates data packets from the sender, to ensure that data is not tampered during transmission.
- The IPsec receiver authenticates whether the sender that sends IPsec packets is valid.
- Anti-replay: The IPsec receiver detects and rejects expired or repetitive packets.

The Internet Key Exchange (IKE) protocol can be configured to provide IPsec with services of automatically negotiating exchange keys and establishing and maintaining Security Associations (SAs), so as to simplify the IPsec application and management. IKE negotiation is not mandatory. The policies and algorithms used by IPsec can be manually configured.

IPsec Implementation

IPsec implements security services via the following protocols:

- Authentication Header (AH): This protocol is numbered 51, and mainly provides data authentication, data integrity check, and anti-replay functions. It supports Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), and so on. An AH packet header is placed behind the standard IP header, to ensure the integrity and authenticity of data packets, and prevent hackers from intercepting data packets or inserting forged data packets to a network.
- Encapsulating Security Payload (ESP): This protocol is numbered 50. Different from AH, ESP encrypts user data to be protected and then encapsulates the data into the IP packets to ensure the data confidentiality. The encryption algorithms supported by ESP include the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and so on. Moreover, the MD5 and SHA-1 algorithms are optional and can be selected to ensure the packet integrity and authenticity, which is optional.

AH and ESP can be used separately or jointly. When the device uses AH and ESP jointly, the device conducts ESP encapsulation on a packet and then conducts AH encapsulation. The encapsulated packet is composed of the original IP packet, ESP header, AH header, and external IP header from inside out.

Protocols and Standards

- 2401 Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998. (Format: TXT=168162 bytes) (Obsoletes RFC1825) (Obsoleted by RFC4301) (Updated by RFC3168) (Status: PROPOSED STANDARD)

- 2402 IP Authentication Header. S. Kent, R. Atkinson. November 1998. (Format: TXT=52831 bytes) (Obsoletes RFC1826) (Obsoleted by RFC4302, RFC4305) (Status: PROPOSED STANDARD)
- 2403 The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13578 bytes) (Status: PROPOSED STANDARD)
- 2404 The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13089 bytes) (Status: PROPOSED STANDARD)
- 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy. November 1998. (Format: TXT=20208 bytes) (Status: PROPOSED STANDARD)
- 2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998. (Format: TXT=54202 bytes) (Obsoletes RFC1827) (Obsoleted by RFC4303, RFC4305) (Status: PROPOSED STANDARD)
- 3948 UDP Encapsulation of IPsec ESP Packets. A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg. January 2005. (Format: TXT=30366bytes) (Status: PROPOSED STANDARD)

1.2 Applications

N/A

1.3 Features

Basic Concepts

↘ Security Association (SA)

IPsec provides secure communication between two end points. The end points are called IPsec peers.

SAs are the basis and essence of IPsec. An SA specifies elements agreed between communication peers. For example, an SA specifies the protocol to be used (AH, ESP, or both), protocol encapsulation mode (transport mode or tunnel mode), encryption algorithm (DES, 3DES, or AES), shared key of protected data in specific flows, and key lifetime.

An SA is unidirectional. In the bidirectional communication between two peers, at least two SAs are required to protect data flows in both directions. In addition, if both peers need to use both AH and ESP to ensure secure communication, each peer establishes an independent SA for each protocol.

An SA is uniquely identified by a triplet. The triplet includes the Security Parameter Index (SPI), destination IP address, and security protocol ID (AH or ESP).

SPI is a 32-bit value generated for uniquely identifying an SA. It is placed in the AH header and ESP header for transmission. When an SA is manually configured, you need to manually specify the SPI. When an SA is established by means of IKE negotiation, SPI is randomly generated.

An SA has a lifetime and only SAs that are established via IKE negotiation have lifetime. SAs are classified into two types:

- Time-based SAs. A time-based SA defines the duration from establishment to the expiration of an SA.
- Traffic-based SAs. A traffic-based SA defines the maximum traffic that can be processed by an SA.

When the lifetime of an SA reaches the specified time or traffic, the SA will expire. Before an SA expires, IKE negotiates and establishes a new SA for IPsec. In this way, a new SA is available before the old SA expires. The old SA is still used to protect communication before a new SA is agreed on. After the new SA is agreed on, the new SA will be immediately used to protect communication.

Encapsulation Mode

IPsec supports two work modes:

- Tunnel mode: In this mode, an entire IP packet is used to calculate the AH header or ESP header. The AH header or ESP header and user data encrypted using ESP are encapsulated into a new IP data packet. The tunnel mode is usually applied to the communication between two security gateways.
- Transport mode: In this mode, only transport-layer data is used to calculate the AH header or ESP header. The AH or ESP header and user data encrypted using ESP are placed behind the original IP header. The transport mode is usually applied to the communication between two hosts, or between one host and one security gateway. It cannot be used to protect forwarded data.

Authentication Algorithm and Encryption Algorithm

(1) Authentication algorithm

The authentication algorithm is implemented using the hash function. The hash function is an algorithm that allows input of messages of any length and generates output of a fixed length. The output is called message digest. Both IPsec peers calculate the message digests. If two message digests are the same, it indicates that packets are complete and are not tampered. IPsec uses two authentication algorithms:

- MD5: Generates a 128-bit message digest via the input message of any length.
- SHA-1: Generates a 160-bit message digest via the input message of less than 264 bits.

The MD5 algorithm is faster than the SHA-1 algorithm in calculation speed but poorer in security strength.

(2) Encryption algorithm

The encryption algorithm is implemented using the symmetric key system. It uses the same key to encrypt and decrypt data. IPsec supports three encryption algorithms:

- DES: Uses a 56-bit key to encrypt a 64-bit plaintext block.
- 3DES: Use three 56-bit DES keys (totaling 168 bits) to encrypt the plaintext.
- AES: Uses a key of 128 bits, 192 bits, or 256 bits to encrypt the plaintext.

The security ranking of the three encryption algorithms is AES, 3DES, DES in descending order. The implementation mechanism of an encryption algorithm with high security is complex and the operation speed is slow. The DES algorithm can meet common security requirements.

Negotiation Mode

SAs can be established in two negotiation modes:

- The manual mode is complex. All information required for creating an SA must be manually configured, and the manual mode does not support some advanced features (such as periodical key update). Nevertheless, this mode can implement the IPsec function separately without relying on the IKE.

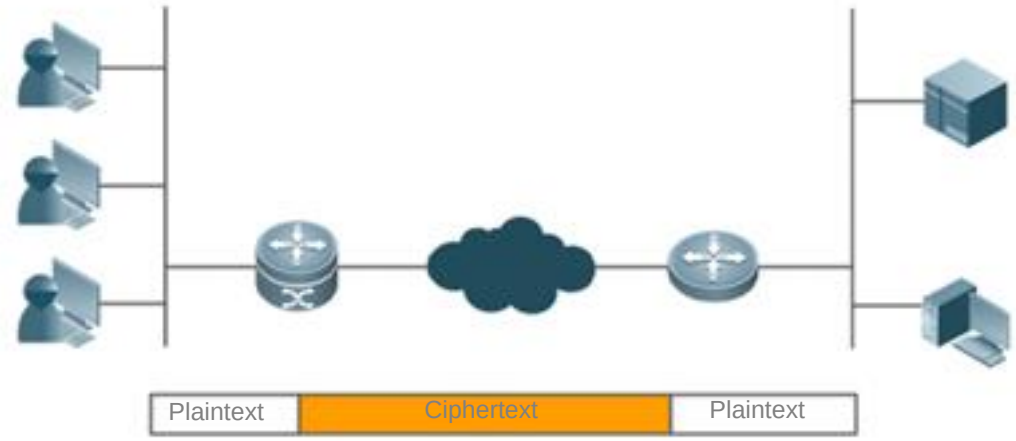
- The IKE automatic negotiation mode, in which the Internet Security Association and Key Management Protocol (ISAKMP) is used, is relatively simple. After an IKE negotiation security policy is configured, IKE automatically negotiates to establish and maintain SAs.

When a few peers communicate with the device or in a small-sized static environment, SAs can be manually configured. For large- and medium-sized dynamic network environments, IKE negotiation is recommended for establishing SAs.

Security Tunnel

A security channel is an interconnection channel established between the local end and the peer end. It consists of one or more SA pairs.

Figure 1-1 shows an example of IPsec protection implemented between subnets.



Requirement for the IPsec model: Interested flows are matched by priority during detection. IPsec cannot process the conflict occurring in interested flows.

Overview

Features	Description	
IPsec Tunnel	Configuring the Default Lifetime	Ensures key security. The tunnel key needs to be updated periodically and the update interval can be changed by configuring the lifetime.
	Configuring the DF Bit Override Functionality for an IPsec Tunnel	Controls the Don't Fragment (DF) bit after tunnel encapsulation.
	Creating a Crypto ACL	Encapsulates interesting traffic in the tunnel. Only data in interesting traffic is encapsulated.
	Defining a Transform Set	Defines the encapsulation format and relevant algorithms.
	Creating a Crypto Map Entry	Defines a tunnel feature set.

	Configuring a Multicast Policy	Configures a multicast policy. According to RFC protocols, tunnels do not support multicast packets. Some devices do not filter out multicast packets but adjust the encapsulation logic as required to achieve compatibility.

1.3.1 IPsec Tunnel

Working Principle

You can create common manual tunnels by configuring some static policies on the CLI.

In the establishment of a tunnel using ISAKMP auto-negotiation, an encryption tunnel is established using IKE (described in the chapters below) and then an IPsec tunnel is negotiated using the IKE tunnel. The IKE tunnel is independent of the IPsec tunnel, and they are not directly associated. After the IKE tunnel is deleted, the IPsec tunnel can still exist. After the IPsec tunnel is deleted, the IKE tunnel can still exist. Therefore, IPsec tunnel-relevant control is effective only to IPsec tunnels.

Related Configuration

↘ Configuring Default Lifetime

This configuration is optional. You can use this command to change the default lifetime of the system. IKE uses this lifetime for negotiation unless otherwise specified, to ensure that the IPsec lifetime does not exceed the default lifetime.

The default lifetime of the system is 1 hour (3,600 seconds) or 4,608,000 KB of communication amount (that is, the communication lasts 1 hour at the rate of 10 MB per second). You can skip this step if you allow the default value. The default lifetime is used if no special description is provided in encryption mapping entries. When negotiating the IPsec lifetime, IKE uses the smaller value of the lifetime on the local peer and remote peer. When the lifetime of an IPsec SA expires, the IKE re-negotiates the IPsec SA and uses new parameters and keys for the IPsec SA so that the IPsec SA functions properly.

An SA and relevant keys time out upon the expiration of the lifetime that expires first. The lifetime is specified using the number of seconds (specified by the **seconds** keyword) or transmission communication amount in KBs (specified by the **kilobytes** keyword).SAs that are manually established (using the encryption mapping entry marked with **IPsec-manual**) have no lifetime limitations.

To ensure that a new SA is ready for use when the old SA expires, the new SA must be negotiated prior to the timeout of the old SA. A new SA is negotiated 30 seconds before the lifetime of the old SA expires or when the communication amount of the channel is 256 bytes apart from the lifetime (depending on the communication peer of which the SA lifetime expires first).

If no communication data passes through a channel during the lifetime of the SA, the SA will be released and no new SA will be negotiated when the lifetime expires. A new SA will be negotiated only when a packet needs to be protected by IPsec for transmission.

ⓘ The default lifetime configuration of the system does not need to be changed. It needs to be changed only in special scenarios.

The lifetime can be globally configured or configured for a specific encryption mapping set.

Configuring DF Bit Coverage Function for IPsec Tunnel

Set whether fragmentation is allowed for IP packets encapsulated using IPsec.

The DF bit coverage function allows a customer to specify whether the device sets the DF bit to 0 or 1, and copies the encapsulated packer header.

The DF bit in the IP packet header determines whether the device allows fragmentation. The value **1** indicates packets cannot be fragmented and the value **0** indicates packets can be fragmented. In IPsec tunnel mode, this function enables the device to control, globally or at the interface layer, whether the DF bit in the IP header encapsulated by IPsec is determined based on the DF bit value in the original IP header. This function is supported only in tunnel mode.

The device performs the zero-out operation by default, indicating that fragmentation is allowed. This function needs to be configured in scenarios with special requirements.

This function can be configured globally only.

Creating Encryption Access List

An encryption access list is used to specify the data flows to be protected by the device. IPsec filters incoming and outgoing packets according to the encryption access list. It protects outgoing data that matches the encryption access list, and checks the validity of incoming packets that match the encryption access list.

An encryption access list is actually a common ACL, and is referenced in encryption mapping entries. An encryption access list is mandatory in static configuration mode. In dynamic mode, an encryption access list can be learnt; in profile mode, no encryption access list needs to be configured, but L2TP over IPsec is applied to encrypt L2TP tunnel packets.

The encryption access list specified in IPsec encryption mapping entries supports the four functions below:

- The encryption access entry that references the deny configuration in the ACL is not used for tunnel negotiation but used as special configuration. Data that meets the entry will not be encrypted.
- The encryption access list screens the outbound communication data to be encrypted and protected by IPsec (permit = protection). The image screening policy is automatically generated and it does not need to be configured in both directions.
- When the negotiation of an IPsec SA starts, the encryption access list specifies the data flows to be protected by the new SA.
- In the processing of inbound communication, the encryption access list is used to filter out and discard communication data that should have been protected by IPsec.
- When IKE negotiation initiated by IPsec peers is processed, the encryption access list is used to determine whether to allow the application for an IPsec SA for interested flows (negotiation is required only for IPsec ISAKMP encryption mapping entries). The ACLs at both peers must be matched. It is recommended that ACLs at both peers be the same.

IPsec filters incoming and outgoing packets according to the encryption access list. It protects outgoing data that matches the encryption access list, and checks the validity of incoming packets that match the encryption access list. Each encryption mapping set is used to protect a different interested flow on the

same interface and the encryption mapping set configuration cannot conflict. Otherwise, the tunnel configured later cannot forward data.

Interested flows do not need to be configured only in dynamic mode. It is mandatory in other cases.

Defining Transformation Set

A transform set is used to instruct a device how to protect data flows. A transformation set is a combination of specific security protocols and algorithms. It specifies the algorithm, security protocol, and data encapsulation mode. You need to specify the protection degree and requirements in a transform set first.

The following table describes all transformation sets supported by the system.

Algorithm Combination	Description
ah-md5-hmac	AH protocol and MD5 HMAC authentication algorithm
ah-sha-hmac	AH protocol and SHA HMAC authentication algorithm
ah-sm3-hmac	AH protocol and SM3 HMAC authentication algorithm
esp-des	ESP protocol and DES encryption algorithm
esp-3des	ESP protocol and 3DES encryption algorithm
esp-aes-128	ESP protocol and AES encryption algorithm using a 128-bit key
esp-aes-192	ESP protocol and AES encryption algorithm using a 192-bit key
esp-aes-256	ESP protocol and AES encryption algorithm using a 256-bit key
ah-md5-hmac esp-des	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol and DES encryption algorithm inside
ah-sha-hmac esp-des	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol and DES encryption algorithm inside
ah-md5-hmac esp-des esp-md5-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-md5-hmac esp-null esp-md5-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-md5-hmac esp-des esp-sha-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-md5-hmac esp-null esp-sha-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and SHA HMAC authentication algorithm inside
ah-sha-hmac esp-des esp-md5-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-sha-hmac esp-null esp-md5-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and MD5 HMAC authentication algorithm inside

ah-sha-hmac esp-des esp-sha-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-sha-hmac esp-null sp-sha-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and SHA HMAC authentication algorithm inside
esp-des esp-md5-hmac	ESP protocol, DES encryption algorithm, and MD5 HMAC authentication algorithm
esp-null esp-md5-hmac	ESP protocol, zero encryption algorithm, and MD5 HMAC authentication algorithm
esp-des esp-sha-hmac	ESP protocol, DES encryption algorithm, and SHA HMAC authentication algorithm
esp-null esp-sha-hmac	ESP protocol, zero encryption algorithm, and SHA HMAC authentication algorithm
esp-3des	ESP protocol and 3DES encryption algorithm
esp-3des esp-sha	ESP protocol, 3DES encryption algorithm, and SHA HMAC authentication algorithm
esp-3des esp-md5	ESP protocol, 3DES encryption algorithm, and MD5 HMAC authentication algorithm
ah-md5-hmac esp-des	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol and 3DES encryption algorithm inside
ah-sha-hmac esp-des	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol and 3DES encryption algorithm inside
ah-md5-hmac esp-3des esp-sha	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-sha-hmac esp-3des esp-sha	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-md5-hmac esp-3des esp-md5	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-sha-hmac esp-3des esp-md5	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and MD5 HMAC authentication algorithm inside

- In general, the esp-des combination (no data authentication) can meet the requirements. If you need to authenticate data, you can use esp-des esp-md5-hmac or esp-des esp-sha-hmac.
- A transformation set is mandatory and can be referenced in multiple encryption mapping sets. Multiple transformation sets can be configured for one encryption mapping set. Transformation sets are matched by priority, and repetitive content of transformation sets does not affect negotiation results.

Creating Encryption Mapping Entry

An encryption mapping entry is used to associate the predefined ACL with transformation sets and define keys and peer addresses to form a complete IPsec solution description.

- An encryption mapping set is mandatory and can be referenced by multiple interfaces.

Configuring Multicast Policy

A multicast policy is used to disable IPsec encapsulation on multicast and broadcast packets.

By default, packets are encrypted when they meet the interested flows configuration, regardless of whether they are multicast packets.

The configuration is optional.

Applying Encryption Mapping Entry to Interface

Activate a defined IPsec scheme. Apply an encryption mapping entry to an interface so that the encryption mapping set works on the interface.

Creating Profile Encryption Mapping Entry

Create a profile encryption mapping entry for establishing an SA using IKE.

Applying Profile Encryption Mapping Entry to Tunnel Interface

Apply a profile encryption mapping set to a tunnel interface.

Activate a tunnel after the configuration is applied to the tunnel interface. The tunnel does not affect data forwarding prior to tunnel activation.

An encryption mapping set can be applied only to a Layer-3 interface. It cannot be configured on Layer-2 ports such as the switching port.

Applying a Profile Crypto Map Entry to a Tunnel Interface

Applies a profile crypto map set to a tunnel interface.

Activate a tunnel after the configuration is applied to the tunnel interface. The tunnel does not affect data forwarding before tunnel activation.

A crypto map set can be applied only to a Layer 3 interface. It cannot be configured on Layer 2 interfaces such as switch interfaces.

1.4 Configuration

Configuration	Description and Command	
Configuring IPsec	**crypto IPsec security-association lifetime**	Configures the default lifetime.
	crypto IPsec df-bit	Configures the DF bit coverage function for the IPsec tunnel.
	access-list	Creates an encryption access list.
	crypto IPsec transform-set	Defines a transformation set.
	crypto map **crypto IPsec profile**	Creates an encryption mapping entry.
Applying IPsec	**crypto map**	Applies IPsec to an interface.

1.4.1 Configuring IPsec

Configuration Effect

- Configure IPsec tunnel negotiation function for establishing a tunnel.

Notes

- The negotiation will not be initiated if the configuration is incomplete.
- In transport mode, interested flows must be host-to-host traffic. Otherwise, the negotiation is automatically conducted in tunnel mode.
- The interested flow conflict cannot be detected. In static configuration mode, interested flows are matched by the configuration sequence; in dynamic mode, a tunnel established later has a higher priority than a tunnel established earlier.

Configuration Steps

↘ (Optional) Configuring Default Lifetime

- This configuration is optional. You can use this command to change the default lifetime of the system. IKE uses this lifetime for negotiation unless otherwise specified, to ensure that the IPsec lifetime does not exceed the default lifetime.
- The default lifetime configuration of the system does not need to be changed. It needs to be changed only in special scenarios.
- The lifetime can be globally configured or configured for a specific encryption mapping set.

↘ (Optional) Configuring DF Bit Coverage Function for IPsec Tunnel

- Set whether fragmentation is allowed for IP packets encapsulated using IPsec.
- The device performs the zero-out operation by default, indicating that fragmentation is allowed. This function needs to be configured in scenarios with special requirements.
- This function can be configured globally only.

↘ Creating Encryption Access List

- An encryption access list is used to specify the data flows to be protected by the device. IPsec filters incoming and outgoing packets according to the encryption access list. It protects outgoing data that matches the encryption access list, and checks the validity of incoming packets that match the encryption access list. Each encryption mapping set is used to protect a different interested flow on the same interface and the encryption mapping set configuration cannot conflict. Otherwise, the tunnel configured later cannot forward data.
- Interested flows do not need to be configured only in dynamic mode. It is mandatory in other cases.
- When interested flow configuration references an extended ACL, it is referenced in the encryption mapping set.

↘ Defining Transformation Set

- A transform set is used to instruct a device how to protect data flows. A transformation set is a combination of specific security protocols and algorithms. It specifies the algorithm, security protocol, and data encapsulation mode. You need to specify the protection degree and requirements in a transform set first.
- A transformation set is mandatory and can be referenced in multiple encryption mapping sets. Multiple transformation sets can be configured for one encryption mapping set. Transformation sets are matched by priority, and repetitive content of transformation sets does not affect negotiation results.

↘ Creating Encryption Mapping Entry

- An encryption mapping entry is used to associate the predefined ACL with transformation sets and define keys and peer addresses to form a complete IPsec solution description.
- An encryption mapping set is mandatory and can be referenced by multiple interfaces.

Verification

- Run the **show crypto map** command to display the configuration integrity. If information is displayed, it indicates that the configuration is complete.
- Run the **show crypto transform-set** command to display the configuration.
- Run the **show crypto map detail** command to display the configuration.

Related Commands

↘ Configuring Default Lifetime

Command	**crypto IPsec security-association lifetime** { **seconds** *seconds* | **kilobytes** *kilobytes* }
Description	seconds Indicates the SA timeout time (unit: seconds). The default value is **3,600** seconds (1 hour). It can be set to **0**, indicating that the time timeout function is disabled. *Kilobytes*: Indicates the SA timeout communication amount (unit: KB). The default value is **4,608,000** KB. It can be set to **0**, indicating that the byte timeout function is disabled.
Command Mode	Global configuration mode
[Upgrade Guide];	N

↘ Configuring the IPsec SA Detection Interval (Optional)

Command	**crypto IPsec security-association detect** *second*
Parameter Description	*second*: Indicates the SA detection interval in seconds
Command Mode	Global configuration mode
Usage Guide	SA detection is disabled by default. When a tunnel exists but data cannot be transmitted, IPsec peers fail to negotiate again. You can run this command to detect whether data transmission is normal. If not, reestablish an SA.

↘ Configuring the Termination Time of an Aged IPsec SA (Optional)

Command	**crypto IPsec security-association expire-time** *second*
Parameter Description	*second*: Indicates the termination time of an aged IPsec SA. The default value is **30**s.
Command Mode	Global configuration mode
Usage Guide	When IPsec peers establish a new SA, the default termination time of an aged SA is 30s. This helps a device switch to a new SA fast when the device works with a competitor's device and the switching mechanisms are different.

Configuring the Matching Rule for IPsec Phase 2 Lifetime Negotiation and Taking the Smaller One of the Lifetimes Configured on Devices In HQ and Branches as the Negotiation Result (Optional)

Command	**crypto IPsec security-association lifetime not_based_on initiator**
Parameter Description	*NA*
Command Mode	Global configuration mode
Usage Guide	The phase 2 lifetime negotiation result is subject to the lifetime configured on the device in the branch by default. That is, both the device in HQ and the device in the branch use the value configured on the device in the branch as the phase 2 lifetime. You can modify the matching rule for phase 2 lifetime negotiation. That is, use the smaller one of the lifetimes configured on devices in the HQ and branch as the final negotiation result.

Disabling Packet Retransmission Check (Optional)

Command	**crypto IPsec security-association replay disable**
Parameter Description	*NA*
Command Mode	Global configuration mode
Usage Guide	After packet retransmission check is disabled, IPsec does not check retransmitted packets. This improves packet processing efficiency but increases the risk of denial of service (DoS) attacks.

Configuring DF Bit Coverage Function for IPsec Tunnel

Command	**crypto IPsec df-bit** { **clear** | **set** | **copy** }
Parameter Description	**clear**: Zeroes out the DF bit in the external IP header. The device may fragment packets and encapsulate the data via IPsec. **clear** is the default value **set**: Sets the DF bit to 1 in the external IP header. If the DF bit in the original IP header is zeroed out, the device may fragment packets. **copy**: Uses the original DF bit value as the DF bit value of the external header. The default value is **copy**.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating Encryption Access List

Command	**access-list** *access-list-number* { **deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
Parameter Description	**deny**: Ignores the target flow. **permit**: Allows the target interested flow. *protocol*: Indicates the protocol. *source source-wildcard*: Indicates the source IP address or network segment of the interested flow. *destination destination-wildcard*: Indicates the destination IP address or network segment. **log**: Enables the ACL log function.
Command Mode	Global configuration mode
Usage Guide	Describe the data flows via the source address, destination address, wildcard, communication protocol, and communication interface of the data flows. The **permit** keyword enables all IP communication that meets specified conditions to be encrypted and protected by the policy described in encryption mapping entries. The **deny** keyword exempts communication data from encryption and protection specified in specific encryption mapping entries.

Defining Transformation Set

Command	**crypto IPsec transform-set** *transform-set-name transform1 [transform2 [transform3]]*
Parameter Description	*transform-set-name*: Indicates the name of an encryption transformation set. *transform1, transform2, transform3*: Indicates the encryption mode and authentication mode.
Command Mode	Global configuration mode
Usage Guide	1. A set is a combination of security protocols, algorithms, and other settings of communication protected by IPsec. During IPsec SA negotiation, peers must use the same specific transformation set to protect specific data flows. 2. Configure multiple transformation sets and then specify one or several of them in the encryption mapping entries. Transformation sets defined in encryption mapping entries are used to negotiate IPsec SAs, so as to protect data flows that match the ACL referenced in encryption mapping entries. During negotiation, both peers search for the same transformation set that is available on both peers. When such a transformation set is found, it is selected as a part of IPsec SAs of both peers and applied to protected communication data. 3. If an SA is configured manually, no parameter needs to be negotiated for the SA. Therefore, the same transformation set must be specified on both peers.
Command	**mode** { **transport** | **tunnel** }
Parameter Description	**transport**: Indicates the transport mode. **tunnel**: Indicates the tunnel mode.
Command Mode	Encryption transformation set definition mode
Usage Guide	Mode setting is effective only to communication using addresses of IPsec peers as source and destination addresses. Other communication is made in tunnel mode. If the source and destination addresses of the communication to be protected are those of IPsec peers and the transport mode is specified, the device requests the transport mode during negotiation but can accept both the transport mode and tunnel mode. If the tunnel mode is

	specified, the device requests the tunnel mode and accepts only the tunnel mode.

Creating Encryption Mapping Entry

Command	**crypto map** *map-name seq-num* **IPsec-isakmp** **crypto IPsec profile** *profile-name*
Parameter Description	*map-name*: Indicates the name of an encryption mapping set. *seq-num*: Indicates the priority of the encryption mapping set. *profile-name*: Specifies that there is no priority in profile mode.
Command Mode	Global configuration mode
Usage Guide	Mandatory parameters of an IPsec tunnel are configured in encryption mapping set mode. Configure the peer address, encryption transformation set, and interested flow to be referenced. **Isakmp-peer**: Specifies the peer and the source interface. **match address**: Specifies the access list for the encryption mapping entry. **set local**: Specifies the local IP address in the encryption mapping entry. **set peer**: Specifies the IP address of the remote peer. **set transform-set**: References the encryption transformation set. **reverse-route**: Configures the reverse route.

Command	**match address** *access-list-numberid*
Parameter Description	*access-list-numberid*: Number of an ACL (100-199, 2000-2699, and 2900-3899). Crypto maps use only IP extended ACLs.
Command Mode	Crypto map configuration mode
Usage Guide	Specify an ACL for a crypto map entry. A crypto map entry uses an ACL to specify data to be protected by IPsec. The ACL specified by this command is applied to both outbound and inbound communication data. If it is detected that outbound data matches an ACL and an SA is established, the device encrypts and forwards the data. If no SA is established, the device triggers the IKE SA negotiation. If it is detected that inbound data matches an ACL, the device decrypts encrypted data and discards unencrypted data.

Command	**match any**
Parameter Description	N/A
Command Mode	Crypto map configuration mode
Usage Guide	The command is used to specify the interesting traffic with the local IP address/mask (0.0.0.0/0.0.0.0) and peer IP address/mask (0.0.0.0/0.0.0.0) in a profile crypto map set. This profile is mainly used for IPsec over Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (l2tp) over IPsec. If the **match any** command is configured in a profile used for IPsec over GRE, the interesting traffic negotiated in IPsec phase 2 has the local IP address/mask (0.0.0.0/0.0.0.0) and peer IP address/mask (0.0.0.0/0.0.0.0) *ip-address*: Indicates the local IP address. *local-inf*: Indicates the interface corresponding to the source IP address of the peer.

	out-inf: Indicates the interface that transmits packets.

Command	**set local** *ip-address*
Parameter Description	*ip-address*: Indicates the local IP address.
Command Mode	Crypto map configuration mode
Usage Guide	Specify a remote peer for a crypto map entry. You can configure multiple remote peers. Negotiation is initiated in the configured peer sequence. When the negotiation fails, the next peer IP address will be used for negotiation.

Command	**set peer** { *hostname* | *ip-address* }
Parameter Description	*ip-address*: Indicates the IP address of a remote peer. *hostname*: Indicates the host name of a remote peer.
Command Mode	Crypto map configuration mode
Usage Guide	Specify a remote peer for a crypto map entry. You can configure multiple remote peers. Negotiation is initiated in the configured peer sequence. When the negotiation fails, the next peer IP address will be used for negotiation.

Command	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
Parameter Description	*transform-set-name*: indicates a referenced encryption transformation set.
Command Mode	Crypto map configuration mode
Usage Guide	A transform set is indispensable to establish an SA successfully. Use this command to specify a transform set when you configure a crypto map. You can configure multiple transform sets and select one of them for SA negotiation.

Command	**reverse-route** [**no-peer** | **remote-peer** *ip-address*] [*distance*]
Parameter Description	**no-peer**: Specifies no next-hop address. **remote-peer** *ip-address*: Specifies the next-hop address. The parameter is optional. *distance*: Indicates next-hop distance. The value range is from 1 to 255.
Command Mode	Crypto map configuration mode
Usage Guide	After this function is configured and the negotiation of a tunnel is complete, the IPsec module automatically adds a static route pointing to the peer end of the tunnel or to a specified IP address.

Command	**set autoup**
Parameter Description	N/A
Command Mode	Crypto map configuration mode
Usage	This command can prevent packet loss caused by tunnel negotiation. Use this command when data

Guide	transmission is sensitive and a tunnel needs to keep connected.

Command	**set isakmp-policy** *number*
Parameter Description	*number*: Indicates the sequence number of a specified negotiation policy. The value range is from 1 to 10,000.
Command Mode	Crypto map configuration mode
Usage Guide	In the aggressive mode, a device in the branch sends only the IKE policy with the highest priority to a device in the HQ for negotiation by default. Therefore, if the device in the branch negotiates with multiple devices in the HQ in the aggressive mode, all the IKE policies with the highest priority on the devices in the HQ must be consistent with the IKE policy on the device in the branch, which reduces device compatibility. You can use this function to specify the IKE policy for negotiation for a crypto map. In this way, the IKE policies with the highest priority on the devices in the HQ do not need to be consistent with the IKE policy on the device in the branch. The function takes effect only in a static crypto map and cannot be configured in a dynamic crypto map.

Command	**set mtu** *length*
Parameter Description	*length*: Indicates the size of a data fragment before encapsulation, in bytes. The range is from 512 to 1,500.
Command Mode	Crypto map configuration mode
Usage Guide	After fragmentation is configured in the tunnel mode, you can use this function to configure the size of data fragments before encapsulation. Select an appropriate fragment size based on the MTU value of each interface in the network forwarding path.

Command	**set peer-identical**
Parameter Description	N/A
Command Mode	Crypto map configuration mode
Usage Guide	When a crypto ACL contains multiple ACEs and multiple remote peers are configured in a crypto map, configure this command to ensure that all ACEs are used for negotiation with the same peer.

Command	**set peer-preempt**
Parameter Description	N/A
Command Mode	Crypto map configuration mode
Usage Guide	When multiple remote peers are configured and a remote peer with a higher priority is needed for negotiation, configure this command. You can configure multiple remote peers in a crypto map. The peer configured first has a higher priority. The peer with a higher priority is used first for negotiation. When the tunnel between the device and a peer with the peer is disconnected, the device automatically switches to another peer for

	negotiation. If the peer with a higher priority can initiate negotiation, run this command to use the peer with a higher priority for negotiation and forwarding, and disconnect the tunnel from a peer with a lower priority.

Command	**set pfs** { **group1** | **group2** | **group5** }
Parameter Description	**group1**: Indicates the 768-bit Diffie-Hellman group. **group2**: Indicates the 1024-bit Diffie-Hellman group. **group5**: Indicates the 1536-bit Diffie-Hellman group.
Command Mode	Crypto map configuration mode
Usage Guide	Configure the Diffie-Hellman group identifier for IPsec tunnel encapsulation as required. Group 1, group 2, and group 5 are the 768-bit, 1024-bit, and 1536-bit Diffie-Hellman groups respectively. The security and required computation time of these groups increase in sequence.

Command	**set session-key** { **inbound** | **outbound** } { **ah** *spi hex-key-data* | **esp** *spi* { **cipher** *hex-key-data* [**authenticator** *hex-key-data*] | **authenticator** *hex-key-data* } }
Parameter Description	*spi*: Indicates security parameter index (SPI). *hex*-key-data: Indicates a hexadecimal key.
Command Mode	Crypto map configuration mode
Usage Guide	This command is used for manually created an SA. This command can only be configured in a manually created crypto map.

Configuring the Local Address for IPsec Negotiation

Command	**crypto map** *map-name* **local-address** *interface-type interface-number*
Parameter Description	Indicates the name of an IPsec encryption mapping set. interface-type: Indicates the interface type of the IPsec local address. interface-number: Indicates the interface number of the IPsec local address.
Command Mode	Global configuration mode
Usage Guide	If an encryption mapping set is applied to multiple interfaces but this command is not executed, the RGOS creates an IPsec SA for each interface with the same traffic on the same remote peer. By default, the IP address of an interface to which the encryption mapping set is applied is used as the address of the local peer. After this command is executed to specify the address of the local peer and the same encryption mapping set is applied to multiple interfaces, only one IPsec SA will be created for the interfaces for communication. If a device has multiple interfaces supporting IPsec communication, this command can be used to specify the IPsec local address for ease of management. In this way, the RGOS uses the specified IP address fixedly to communicate with external routers.

Configuring the IPsec MIB

Command	**crypto mib enable**
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	If IPsec MIB nodes need to be accessed, you need to run a CLI command to enable the IPsec MIB function.

Disabling IPsec for Multicast and Broadcast Packets

Command	**crypto IPsec multicast disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If IPsec is not required for multicast and broadcast packets, you can configure this command to disable IPsec.

Disabling IPsec Security Check

Command	**crypto IPsec optional**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	IPsec security check consumes many resources. Disable the feature to save CPU resources. In the Layer 2 Tunneling Protocol (l2tp) over IPsec model, l2tp can be configured to enable IPsec features forcibly, or to allow only packets encrypted by IPsec to pass through. You are advised to use this combination as required.

1.4.2 Applying IPsec

Configuration Effect

- Apply IPsec configuration to an interface so that the device automatically creates tunnel control information.

Notes

- Before IPsec is applied to an interface, all IPsec configuration does not take effect.
- IPsec tunnels can be applied only to Layer-3 interfaces.
- The same encryption mapping set can be applied to multiple interfaces, and the encryption mapping set is separately applied to multiple interfaces is independent.

Configuration Steps

Applying Encryption Mapping Entry to Interface

- Activate a defined IPsec scheme. Apply an encryption mapping entry to an interface so that the encryption mapping set works on the interface. The configuration is mandatory. Encryption mapping entries can be applied only to Layer-3 interfaces.

Verification

- Run the **show crypto IPsec sa** command to display the configuration integrity. If information is displayed, it indicates that the configuration is complete.
- Run the **show crypto map detail** command to display the configuration.

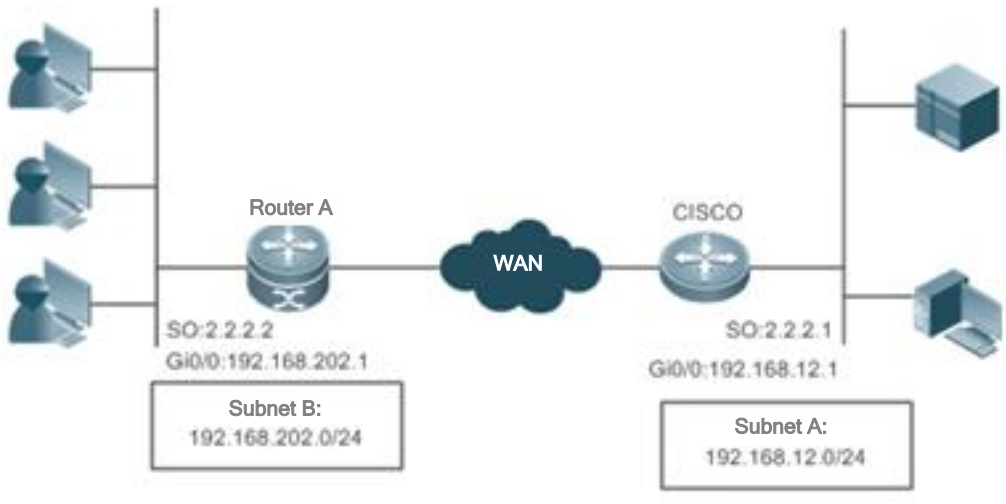
Related Commands

↘ Applying Encryption Mapping Entry to Interface

Command	**crypto map** *map-name*
Parameter Description	*map-name*: Indicates the name of an encryption mapping set.
Command Mode	Interface configuration mode
Usage Guide	Use this command to apply an encryption mapping set to an interface. An encryption mapping set must be applied to an interface so that IPsec encryption and protection can be provided for data on the interface. One interface can be associated with only one encryption mapping set. If multiple encryption mapping entries share the same **map-name** value but different **seq-num** values, these encryption mapping entries belong to the same encryption mapping set and are applied to the same interface. The encryption mapping entry with a smaller **seq-num** value has a higher priority and is used for data matching first.

Configuration Example

↘ Connecting Central Device to Remote Device over IPsec

Scenario Figure 1-2	
Configuration Steps	● An IPsec VPN tunnel is a point-to-point encryption tunnel. Devices at both ends of the tunnel encrypt and decrypt data via the negotiated key. IKE needs to be configured before an IPsec VPN

	tunnel is established. ● **Configuration on Router A:**
Router A	# Enable IKE. Hostname(config)#crypto isakmp enable Hostname(config)#crypto isakmp policy 1 Hostname(isakmp-policy)#authentication pre-share Hostname(isakmp-policy)#encrytiong 3des # Configure a pre-shared key and transformation set. Hostname(config)#crypto isakmp key 0 preword address 2.2.2.1 Hostname(config)#crypto IPsec transform-set myset esp-des esp-md5-hmac # Define an encryption mapping set. Hostname(config)#crypto map mymap 5 IPsec-isakmp Hostname(config-crypto-map)# set peer 2.2.2.1 Hostname(config-crypto-map)# set transform-set myset Hostname(config-crypto-map)# match address 101 # Apply the encryption mapping set to an interface. Hostname(config)#interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.202.1 255.255.255.0 Hostname(config)#interface Serial 0 Hostname(config-if- Serial 0)#ip address 2.2.2.2 255.255.255.0 Hostname(config-if- Serial 0)#encapsulation ppp Hostname(config-if- Serial 0)#crypto map mymap # Define an encryption access list to protect the IP communication between the subnet 192.168.202.0/24 and the subnet 192.168.12.0/24. Hostname(config)#access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
	A tunnel can also be established in manual mode to achieve tunnel encryption. IKE negotiation is not conducted in manual mode and the key is not updated periodically, resulting in poor security and ease of use. # Define a transformation set. Hostname(config)#crypto IPsec transform-set myset esp-des esp-md5-hmac # Define an encryption mapping set. Hostname(config)#crypto map mymap 5 IPsec-manual Hostname(config-crypto-map)# set peer 2.2.2.1 Hostname(config-crypto-map)# set session-key inbound esp 300 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890 Hostname(config-crypto-map)# set session-key outbound esp 301 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890 Hostname(config-crypto-map)# set transform-set myset Hostname(config-crypto-map)# match address 101 # Apply the encryption mapping set to an interface. Hostname(config)#interface GigabitEthernet 0/1

	Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.202.1 255.255.255.0 Hostname(config)#interface Serial 0 Hostname(config-if- Serial 0)#ip address 2.2.2.2 255.255.255.0 Hostname(config-if- Serial 0)#encapsulation ppp Hostname(config-if- Serial 0)#crypto map mymap
	# Define an encryption access list to protect the IP communication between the subnet 192.168.202.0/24 and the subnet 192.168.12.0/24.
	Hostname(config)#access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
	Monitoring and debugging Monitor and debug the SA established using IKE. Send a data packet from any host in Subnet B to Subnet A. IKE negotiation is triggered. An IPsec SA is successfully established. # Enable the IKE and IPsec debugging functions.
	RouterA# debug crypto IPsec IPSEC debugging is on RouterA# debug crypto isakmp ISAKMP debugging is on
	# The following debugging information is displayed during negotiation:
	Get acquire: 192.168.202.0/0.0.0.255 -> 192.168.12.0/0.0.0.255 , prot 0, port 0/0 Acquire negotiate with 2.2.2.1 (36) Beginning Quick Mode exchange, M-ID of 4445127 (36) sending packet to 2.2.2.1 (I) QM_SI1_WR1 IPsec_output:423, get item acclist 101 IPsec_output:429, match 3 (36) received packet from 2.2.2.1 (I) QM_SI1_WR1 payload format: <Hdr>,<hash> <sa> <nonce> <id> (36) processing SA payload. message ID = 4445127 (36) Creating IPsec SAs. inbound SA has spi 4445127 protocol esp, DES_CBC auth MD5 outbound SA has spi 275385850 protocol esp, DES_CBC auth MD5 lifetime of 3600 seconds, soft 3570 seconds lifetime of 4608000 kilobytes, soft 256 kilobytes IPsec_output:423, get item acclist 101 IPsec_output:429, match 3 (36) sending packet to 2.2.2.1 (I) QM_IDLE (36) Phase_2 negotiate complete!
Verification	● To check whether IKE and IPsec SAs are established, run the following commands to display relevant information:
Router A	RouterA# show crypto isakmp sa

destination source state conn-id lifetime(second)
2.2.2.1 2.2.2.2 QM_IDLE 36 5013

The information above shows that an IKE SA is successfully established.

RouterA# show crypto IPsec sa
Interface: Serial0
Crypto map tag:mymap, local addr 2.2.2.2 //The name of the encryption mapping set is mymap and the local address 2.2.2.2 is used.
media mtu 1500
local ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0))
remote ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0))
PERMIT //Protecting the communication between 192.168.202.0/24 and 192.168.12.0/24.
current_peer: 2.2.2.1 //The address of the remote peer is 2.2.2.1.
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#send errors 0, #recv errors 0
//Statistics, which are sequentially the number of encapsulated packets, number of encrypted packets, number of digest packets, number of decapsulated packets, number of decrypted packets, number of verification packets, number of transmission errors, and number of receiving errors.
inbound esp sas: //SA for processing inbound packets. The protocol is ESP.
spi:0x43D3C7 (4445127) //The SPI is 4445127.
transform: esp-des esp-md5-hmac //The transformation set is esp-des-md5.
in use settings={Tunnel,} //The work mode is tunnel mode.
sa timing: remaining key lifetime (k/sec): (4607999/3578)
//The remaining lifetime prior to SA expiration is 4607999 KB/3578 seconds.
IV size: 8 bytes //The IV vector length is 8 bytes.
Replay detection support:Y //Anti-play processing is supported.
outbound esp sas: //SA for processing outbound packets. The protocol is ESP.
spi:0x106A0DFA (275385850) //The SPI is 275385850.
transform: esp-des esp-md5-hmac //The transformation set is esp-des-md5.
in use settings={Tunnel,} //The work mode is tunnel mode.
sa timing: remaining key lifetime (k/sec): (4607999/3577)
//The remaining lifetime prior to SA expiration is 4607999 KB/3577 seconds.
IV size: 8 bytes //The IV vector length is 8 bytes.
Replay detection support:Y //Anti-play processing is supported.

The statistics show that an IPsec tunnel is established and data packets are protected.

Monitor and debug the SA established in manual mode.

The SA manually established starts working without negotiation. The debugging information is not displayed and only statistics can be displayed.

RouterA# show crypto IPsec sa
Interface: Serial0
Crypto map tag:mymap, local addr 2.2.2.2 //The name of the encryption mapping set is mymap and the local address 2.2.2.2 is used.

	media mtu 1500
	local ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0))
	remote ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0))
	PERMIT //Protecting the communication between 192.168.202.0/24 and 192.168.12.0/24.
	current_peer: 2.2.2.1 //The address of the remote peer is 2.2.2.1.
	#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
	#pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
	#send errors 0, #recv errors 0
	//Statistics, which are sequentially the number of encapsulated packets, number of encrypted packets, number of digest packets, number of decapsulated packets, number of decrypted packets, number of verification packets, number of transmission errors, and number of receiving errors.
	inbound esp sas: //SA for processing inbound packets. The protocol is ESP.
	spi: 0x12C (300) //The SPI is 300.
	transform: esp-des esp-md5-hmac //The transformation set is esp-des-md5.
	in use settings={Tunnel,} //The work mode is tunnel mode.
	no sa timing //There is no lifetime.
	IV size: 8 bytes //The IV vector length is 8 bytes.
	Replay detection support:N //There is no anti-play processing.
	outbound esp sas: //SA for processing outbound packets. The protocol is ESP.
	spi: 0x12D (301) //The SPI is 301.
	transform: esp-des esp-md5-hmac //The transformation set is esp-des-md5.
	in use settings={Tunnel,} //The work mode is tunnel mode.
	no sa timing //There is no lifetime.
	IV size: 8 bytes //The IV vector length is 8 bytes.
	Replay detection support:N //There is no anti-play processing.
	The statistics show that an IPsec tunnel is established and data packets are protected.

1.5 Monitoring

Clearing

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

Description	Command
Clears the entire SA database. All active security threads will be deleted.	**clear crypto sa**
Clears the SA with a specific peer address.	**clear crypto sa peer** { *ip-address* | *peer-name* }
Clears the SA of a specific encryption mapping set.	**clear crypto sa map** *map-name*
Clears the SA with a specified <destination address, protocol, and SPI>.	**clear crypto sa spi** *destination-address* { **ah** | **esp** } *spi*

Displaying

Description	Command
Displays the transformation set configuration.	**show crypto IPsec transform-set**

Displays all or specified encryption mapping configuration.	**show crypto map** [*map-name*]
Displays the IPsec SA information.	**show crypto IPsec sa**
Displays the dynamic encryption mapping information.	**show crypto dynamic-map** [*tag map-name*]

Debugging

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

Description	Command
Debugs IPsec events.	**debug crypto IPsec**
Debugs IPsec events.	**debug crypto engine**

2 Configuring IKE

2.1 Overview

In the IP Security (IPSec) implementation, the Internet Key Exchange (IKE) protocol can be used to establish a Security Association (SA). The IKE is established on the framework defined by the Internet Security Association and Key Management Protocol (ISAKMP). IKE provides IPSec with services of automatically negotiating exchange keys and establishing SAs, to simplify IPSec application and management, thereby greatly simplifying the IPSec configuration and maintenance.

IKE does not directly transmit keys in the network but uses a series of exchange data to calculate the key shared by both parties. Even if a third party intercepts all exchange data used for calculating a key, the third party cannot calculate the authentic key.

Functions of IKE in IPSec

- IKE enables IPSec to automatically negotiate many parameters such as the key, thereby reducing the manual configuration complexity.
- During the Diffie-Hellman (DH) exchange of IKE, each calculation is irrelevant to the generated result. The DH exchange is performed during establishment of each SA, which ensures that keys used by SAs are irrelevant.
- IPSec uses the SN in the IP packet header to implement anti-replay. The SN is a 32-bit value. After the value overflows, an SA needs to be re-established to implement anti-replay. This process needs the cooperation of IKE.
- The authentication and management of the identity of each party in secure communication will affect IPSec deployment. The large-scale application of IPSec needs the participation of the Certificate Authority (CA) or other organs that manage identity data in a centralized manner.
- IKE provides end-to-end dynamic authentication.

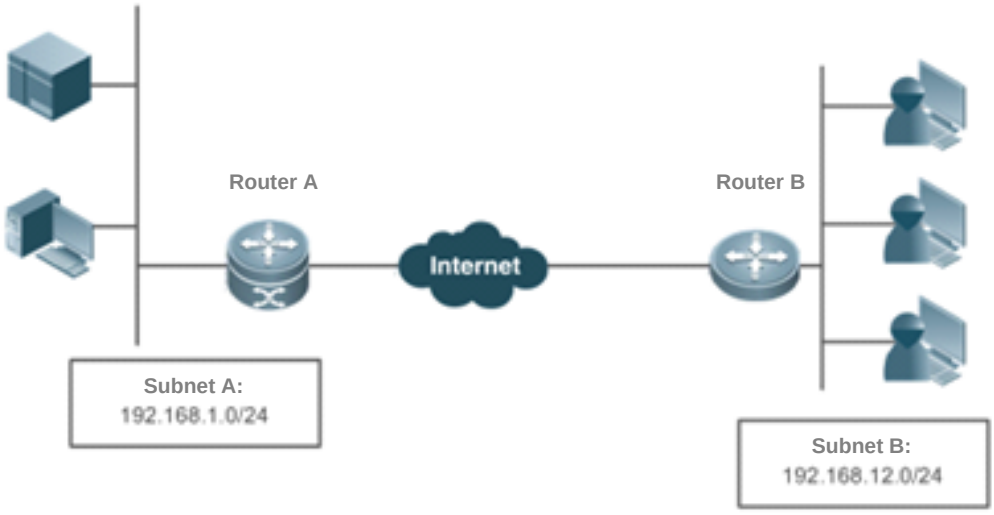
2.2 Applications

2.2.1 Establishing Dynamic VPN Tunnel

Scenario

A VPN tunnel in the star topology is established when the peer IP address is unknown on the convergence side.

Figure 2-1



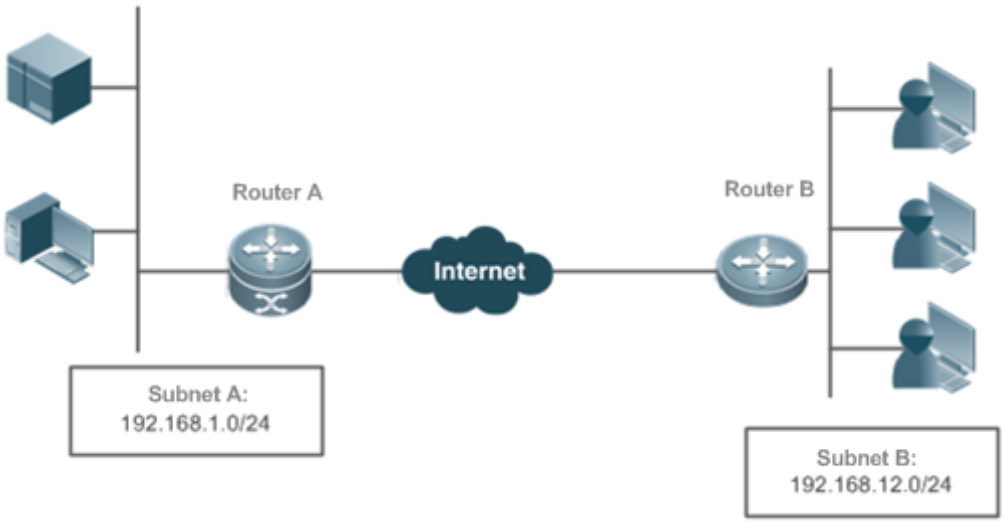
Deployment

- Connect to the WAN over the Asymmetric Digital Subscriber Line (ADSL) or in other modes.
- Establish an IKE tunnel via a public key.
- Implement the internal network routing and interconnection via the IPSec VPN tunnel.
- Establish routes via reverse routing.

2.2.2 Establishing Tunnel via Domain Name

An IKE tunnel is estalbished via a domain name when the server IP address is unknown on the access side.

Figure 2-2



-

Deployment

- Find out the server IP address by means of domain name resolution.
- Query the preset key by using a domain name as the authentication ID, and mutually authenticate devices to establish an IKE tunnel.
- Implement the internal network routing and interconnection via the IPSec VPN tunnel.
- Establish routes via reverse routing.

2.3 Features

IKE Security Mechanism

IKE has a self-protection mechanism, which can securely authenticate identities, distribute keys, and establish IPSec SAs on an insecure network.

1. Data authentication

Data authentication involves two aspects:

- Identity authentication: Identity authentication determines identities of both communication parties. It supports three authentication methods: pre-shared key (pre-shared-key) authentication, PKI-based digital signature (rsa-signature) authentication, and digital email authentication (digital-email).
- Identity protection: Identity data is encrypted for transmission after keys are generated, thereby implementing protection of identity data.

2. DH

Diffie-Hellman (DH) algorithm is a public key algorithm. Both communication parties exchange some data and calculate the pre-shared key when keys are not transmitted. Even if a third party (such as a hacker) intercepts all exchange data used for calculating the key, the third party cannot calculate the authentic key because of high complexity of the DH algorithm. Therefore, the DH exchange technology ensures that both parties securely obtain pubic information.

3. PFS

The Perfect Forward Secrecy (PFS) feature is a security feature, which indicates that the cracking of one key does not affect the security of other keys because these keys have no derivation relationship. IPSec is implemented using one key exchange added in the negotiation of IKE phase 2. The PFS feature is ensured using the DH algorithm.

IKE Exchange Process

IKE negotiates keys and establishes SAs for IPSec in two phases:

(1) Phase 1: Both communication parties establish a channel that passes identity authentication and security protection, that is, establish an ISAKMP SA. In Phase 1, there are two IKE exchange modes: main mode and aggressive mode.

(2) Phase 2: IKE uses the secure channel established in Phase 1 to negotiate the security service for IPSec. That is, IKE negotiates the specific SA used for secure transmission of IP data.

The IKE negotiation in main mode in Phase 1 covers three pairs of messages:

- The first pair is SA exchange messages, which are used to negotiate and determine the relevant security policy.
- The second pair is key exchange messages, which are used to exchange the Diffie-Hellman public value and auxiliary data (such as random number). The key is generated in this phase.
- The last pair is messages that carry ID information and authentication exchange data, which are used to authenticate identities and content exchanged in Phase 1. The major difference between exchange in aggressive mode and that in main mode is as follows: Identity protection is not provided and only three messages are exchanged in aggressive mode. In scenarios with low requirements for identity protection, the aggressive mode, in which a few packets are exchanged, can improve the negotiation speed. The main mode should be used in scenarios with high requirements for identity protection.

Working Principle

IKE is a key management protocol and is used in combination with IPSec. IPSec is an IP security function that provides robust authentication and IP packet encryption. IPSec can be configured without IKE. IKE, however, can provide additional functions and flexibility, and facilitate IPSec configuration, thereby enhancing functions of IPSec. IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE) inside the Internet Security Association and Key Management Protocol (ISAKMP) framework.

IPSec (IKE-reliant IPSec) must be configured and applied to interfaces before IKE starts working. When outgoing data packets that meet requirements are detected on an interface, IPSec triggers IKE to negotiate with IKE of the remote peer. They establish a secure channel between the peers, transmit supported various IPSec parameters, and finally establish consistent SAs at both ends so that IPSec of both parties works properly. When the lifetime of IPSec SAs expires after a period of time, if data that meets requirements needs to be transmitted, the IKE modules of both peers re-negotiate IPSec again and the process repeats.

With IKE, you do not need to manually specify all IPSec parameters and keys in the encryption mapping tables of both communication parties. IKE allows specifying the lifetime of IPSec SAs, enables IPSec to periodically update keys so as to enhance the security, and enables IPSec to provide the anti-replay service.

Overview

Feature	Description
IKE Tunnel	Negotiatie the IKE tunnel establishment

2.3.1 IKE Tunnel

Working Principle

Configure IKE negotiation parameters used for negotiating the IKE tunnel establishment.

Related Configuration

↘ Enabling or Disabling IKE

The IKE function is enabled by default. If you do not want to use IKE and IPSec together, you can run a command to disable the IKE function. In this case, IPSec SAs can be established only in manual mode.

The IKE function is enabled by default. It can be disabled using a command in special cases.

Ensuring Compatibility Between ACL and IKE

IKE is an application that runs over UDP. It uses UDP data packets and Port 500. If an ACL (firewall) is configured on the device to deny the UDP communication packets, the IKE negotiation will fail. Therefore, ensure that communication packets of IKE are not denied.

Creating IKE Policy

Both parties participating in IKE negotiation have at least one consistent IKE policy, which is indispensable for successful IKE negotiation. Multiple prioritized policies must be created on each pair of peers, to ensure that at least one policy matches a policy on the remote peer.

Each IKE policy defines five parameters:

Parameter	Keyword	Optional Value	Default Value
Encryption algorithm	des	56-bit DES-CBC	56-bit DES-CBC
	3des	168-bit 3DES-CBC	
	aes	128-bit AES-CBC	
Hash algorithm	sha	SHA-1 (HMAC variant)	SHA-1 (HMAC variant)
	md5	MD5 (HMAC variant)	
Authentication method	pre-share	Pre-shared key	Digital signature authentication
	rsa-sig	Digital signature authentication	
Diffie-Hellman group identifier	1	768-bit Diffie-Hellman group	768-bit Diffie-Hellman group
	2	1024-bit Diffie-Hellman group	
	5	1536-bit Diffie-Hellman group	
IKE SA lifetime	Null	1 minute to 1 day in seconds	1 day (86,400 seconds)

IKE tries to search for a consistent policy that exists on both peers when starting negotiation. One party that initiates negotiation sends all policies to the remote response party. The remote response party searches policies received from the remote peer by priority for a policy that matches a local policy.

When policies of both parties contain the same encryption algorithm, hash algorithm, authentication algorithm, and Diffie-Hellman parameter values and the lifetime of the policy on the remote peer is shorter than or equal to the lifetime of the compared policy, the shorter lifetime of the policy on the remote peer is used if no lifetime is specified. If no acceptable matched policy is found, IKE rejects negotiation and no IPSec SA is established. If a matched policy is found, IKE completes negotiation and establishes an IPSec SA.

Set parameters to balance between security and performance:

- Encryption algorithm: 56-bit DES-CBC, 168-bit 3DES-CBC, and 128-bit AES-CBC are currently supported.
- Hash algorithm: SHA-1 and MD5. The digest information generated when MD5 is used is less than that generated when SHA-1 is used, and MD5 is usually faster than SHA-1. It is proved that an attack targeted

towards MD5 is successful but the attack method is very difficult. IKE can use the Hashed Message Authentication Code (HMAC) variant (MD5) to defend against such an attack.

- Authentication method: Currently, RGOS supports pre-shared key authentication and digital certificate authentication. In pre-shared key authentication, both parties need to configure correct pre-shared keys. In digital certificate authentication, both parties need to configure correct certificates (see the certificate configuration chapter).
- The Diffie-Hellman group identifier has three options: 768-bit Diffie-Hellman group, 1024-bit Diffie-Hellman group or 1536-bit Diffie-Hellman group. It is difficult to attack the 1024-bit Diffie-Hellman group and the group occupies more CPU resources.
- IKE SA lifetime differs from IPSec SA lifetime. IKE SA lifetime refers to the validity period of IKE parameter negotiation and can be set to any value. As a universal rule, a shorter lifetime (reaching a critical point) indicates more secure IKE negotiation. If a longer lifetime is set, the negotiation of a new IPSec SA is faster.

Multiple IKE policies can be created, and each policy uses the combination of different parameter values. A unique priority (1-10000, with **1** indicating the highest priority) needs to be allocated to each created policy.

Multiple policies can be configured on each pair of peers. Among these policies, ensure that a policy must have the same encryption algorithm, hash algorithm, authentication algorithm, and Diffie-Hellman parameter values (the lifetime can be different) as a policy on the remote peer. If no policy is configured, the device uses the default policy, which is granted the lowest priority and uses the default value of each parameter.

The default policy and default values in configured policies are not displayed in the device configuration. To display the default policy and default values in configured policies, run the **show crypto isakmp policy** command.

By default, the system provides an IKE policy with the lowest priority. For the default configuration, see the chapters below.

Selecting Work Mode

There are two work modes: main mode and active mode (the default mode is main mode).

Configuring Local Identity

Selecting the work mode is specifying the work mode (main mode or active mode) for an initiator to initiate the first negotiation message. In main mode, the local identity configuration does not affect negotiation. In active mode, local identity configuration specifies the identity type in the first negotiation message of the initiator. It directly affects the negotiation in active mode. Currently, the local identity can be configured in three forms: local address; domain name; username@domain name.

By default, the negotiation of a pre-shared key uses an IP address as the ID while digital signature authentication uses the certificate DN as the ID. The digital signature authentication of devices from some other vendors uses an IP address as the ID. In this case, manually specify the ID type to ensure compatibility. There is a case in which the compatibility needs to be modified at the local peer due to the peer configuration. Default values can be used in other cases.

The configuration is valid globally and is not specific to a tunnel.

Configuring Automatic Identification of the Work Mode

A central device needs to support multiple dialup modes (some devices use main mode while some devices use active mode). The central device needs to respond to messages initiated in the two work modes and complete negotiation. Therefore, this command is used in such a work environment and has no effect on initiators.

By default, only negotiation in main mode can be identified because IDs are not protected in aggressive mode and the security in aggressive mode is poorer than that in main mode. Some devices use the aggressive mode for packet transmission by default. Automatic identification of the work mode needs to be configured to achieve compatibility.

Configuring Pre-shared Key

A pre-shared key is a key jointly owned by both peers that participate in IKE negotiation. Therefore, each pre-shared key maps to one pair of IKE peers. On a given peer, a key same as the key owned by multiple remote peers involved in sharing needs to be specified. For security, it is recommended to configure different keys between different peer pairs.

Negotiation of pre-shared keys must be configured. The certificate used in digital signature authentication contains public and private key pairs, which do not need to be configured.

Configuring DPD Detection

Currently, the Dead Peer Detection (DPD) is implemented using two mechanisms: on-demand mechanism and periodic mechanism. In on-demand mechanism, when packets are transmitted after the tunnel idle duration exceeds the configured time, the device is triggered to send a DPD detection message. In periodic mechanism, the device actively sends a DPD detection message after the tunnel idle duration exceeds the configured time. A DPD detection message can be retransmitted for a maximum of five times.

The DPD function is disabled by default. You can set parameters to enable the DPD function. It is recommended to enable the DPD function when the link is unstable.

Setting IKE Negotiation Rate

When thousands of tunnels are negotiated simultaneously, the negotiation fails to converge or the convergence is vslow. As a result, the entire negotiation takes several hours or even longer. To eliminate the deficiency, you can run this command to limit the negotiation rate, to ensure that the number of tunnels that are simultaneously involved in negotiation is controlled to a certain range and improve the negotiation efficiency.

The IKE negotiation rate limit function is enabled by default. The default rate limit is 1000, indicating that a maximum of 1000 tunnels can be simultaneously involved in negotiation. When a large number of tunnels are simultaneously involved in negotiation, if the default rate limit is adopted but the negotiation is still slow or fails, you can adjust the rate limit value. You can also run the **crypto isakmp limit disable** command to disable the negotiation rate limit function.

Setting NAT Traversal Timeout Parameter

The device complies with RFC3947 and uses the IPSEC NAT-T technology and UDP headers to resolve the NAT traversal problem. The keepalive mode is used for transmitting packets to prevent NAT connection timeout. The default time (5 minutes) is used when the NAT traversal timeout parameter is not set.

The NAT traversal function is automatically judged by the protocol and the default parameter value is provided. The value of the NAT traversal timeout parameter needs to be changed according to the NAT

configuration. When no data is transmitted, the keepalive mode ensures that the NAT records are effective, to prevent tunnel data transmission interruption caused by interface re-assignment during NAT re-establishment.

2.4 Configuration

Configuration	Description and Command	
Configuring IKE	**crypto isakmp aggressive-encrypt enable**	Enables encryption for the third packet used in the negotiation in aggressive mode
	crypto isakmp enable	Enables or disables IKE.
	crypto isakmp policy *priority*	Creates an IKE policy.
	crypto isakmp nat-traversal disable	Disables the NAT traversal function.
	crypto isakmp peer { bind | random }	Specifies the first peer that initiates negotiation in the case of multiple peers.
	crypto isakmp session limit *numbers*	Configures the limit on the number of IKE negotiations.
	crypto isakmp nat-traversal disable	Disables the NAT traversal function.
	encryption des | 3des | aes-128 | aes-192 | aes-256	Specifies the encryption algorithm for IKE policies.
	hash {**sha** | **md5**}	Specifies the hash algorithm for IKE policies
	authentication {**pre-share | rsa-sig | digital-email }**	Specifies the authentication method for IKE policies.
	group { **1 | 2 | 5 }**	Specifies the ID of the Diffie-Hellman group in IKE policies.
	lifetime *seconds*	Specifies the lifetime of IKE SAs.
	set exchange-mode { **main | aggressive** }	Sets the work mode used in Phase 1 of IKE negotiation between peers.
	set autoup	Sets tunnel auto-connection.
	set isakmp-policy *number*	Specifies a policy for negotiating a mapping set.
	set local *ip-address*	Specifies the local IP address in an encryption mapping entry.
	set mtu *length*	Sets the IPSec pre-fragmentation mode (valid in tunnel mode)
	set peer { *hostname* | *ip-address* }	Specifies a remote peer in an encryption mapping entry.
	set peer-identical	Specifies multiple ACEs to use the same remote peer in the negotiation in Phase 2.
	set peer-preempt	Specifies the remote peer of a higher priority to initiate preemption

	set pfs { **group1 | group2** }	Specifies the Diffie-Hellman group ID used in IPSec tunnel encapsulation.
	set security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes*] }	Sets the global lifetime used for IPSec SA association in an encryption mapping set.
	reverse-route [**remote-peer** *ip-address* | **no-peer**] [***distance***]	Enables the reverse route injection function
	self-identity	Configures the local identity.
	crypto isakmp mode-detect	Configures automatic identification of the work mode.
	crypto isakmp key	Configures a pre-shared key.
	crypto isakmp keepalive	Configures DPD detection.
	crypto isakmp limit rate	Sets the IKE negotiation rate.
	crypto isakmp nat	Sets the NAT traversal timeout parameter.

2.4.1 Configuring IKE

Configuration Effect

- Configure an IKE negotiation policy.

Notes

- The priorities of IKE policies are sorted by the policy number.
- The default policy number is 65535 and the default policy is used when no policy is configured.

Configuration Steps

- (Optional) Enabling or Disabling IKE Ensure that IKE is working and is not disabled.
- The IKE function is enabled by default. It can be disabled using a command in special cases.

↘ Ensuring Compatibility Between ACL and IKE

- If an ACL is configured on the device, ensure that the device does not prohibit IKE communication data.
- If a conflict causes an abnormality in forwarding of tunnel data and the system cannot identify the abnormality, configuration personnel needs to ensure the compatibility between ACL and IKE.

↘ Creating IKE Policy

- Specify parameters used by IKE. An IKE policy is configured globally.
- By default, the system provides an IKE policy with the lowest priority. For the default configuration, see the chapters below.

↘ Selecting Work Mode

- IKE supports two work modes during IKE negotiation: main mode and active mode (active mode is also called aggressive mode in some documents).
- In aggressive mode, IDs are not protected and fewer packets are involved in negotiation. Select a proper work mode as required.

(Optional) Configuring Local Identity

- Configure the local identity for IKE negotiation.
- By default, the negotiation of a pre-shared key uses an IP address as the ID while digital signature authentication uses the certificate DN as the ID. The digital signature authentication of devices from some other vendors uses an IP address as the ID. In this case, manually specify the ID type to ensure compatibility. There is a case in which the compatibility needs to be modified at the local peer due to the peer configuration. Default values can be used in other cases.
- The configuration is valid globally and is not specific to a tunnel.

Configuring Automatic Identification of the Work Mode

- Configure whether the response party of IKE negotiation automatically accepts negotiation in active mode.
- By default, only negotiation in main mode can be identified because IDs are not protected in aggressive mode and the security in aggressive mode is poorer than that in main mode. Some devices use the aggressive mode for packet transmission by default. Automatic identification of the work mode needs to be configured to achieve compatibility.

Configuring Pre-shared Key

- Configure the joint key between IKE peers. A pre-shared key can be configured for a specific IP address or domain name. Wildcard keys are supported.
- Negotiation of pre-shared keys must be configured. The certificate used in digital signature authentication contains public and private key pairs, which do not need to be configured.

(Optional) Configuring DPD Detection

- DPD detection can be configured in two modes: on-demand mode and periodic mode. It detects whether the peer device functions properly and eliminates tunnel vulnerabilities.
- The DPD function is disabled by default. You can set parameters to enable the DPD function. It is recommended to configure the DPD function when the link is unstable.

(Optional) Setting IKE Negotiation Rate

- Setting the IKE negotiation rate can effectively prevent a negotiation failure or long negotiation duration caused by simultaneous negotiation of a large number of tunnels.
- The IKE negotiation rate limit function is enabled by default. The default rate limit is 1000, indicating that a maximum of 1000 tunnels can be simultaneously involved in negotiation. When a large number of tunnels are simultaneously involved in negotiation, if the default rate limit is adopted but the negotiation is still slow or fails, you can adjust the rate limit value. You can also run the **crypto isakmp limit disable** command to disable the negotiation rate limit function.

(Optional) Setting NAT Traversal Timeout Parameter

- The NAT-T technology uses a UDP header to resolve NAT transversal problem. Keepalive packets need to be used to ensure the persistency of the UDP connection, to prevent NAT connection timeout.
- The NAT traversal function is automatically judged by the protocol and the default parameter value is provided. The value of the NAT traversal timeout parameter needs to be changed according to the NAT configuration. When no data is transmitted, the keepalive mode ensures that the NAT records are effective, to prevent tunnel data transmission interruption caused by interface re-assignment during NAT re-establishment.

Verification

- Run the **show crypto policy** command to check the configuration integrity and whether the configuration is consistent with the peer configuration.

Related Commands

Enabling Encryption for the Third Packet Used in the Negotiation in Aggressive Mode

Command	**crypto isakmp aggressive-encrypt enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When the device interconnects to a partner's device, the device checks whether the third packet is encrypted for the negotiation in aggressive mode. If it is not encrypted, the negotiation fails. Therefore, encryption is enabled for the third packet by default. If encryption is not required in some scenarios, you can run the **no crypto isakmp aggressive-encrypt enable** command to disable this function.

(Optional) Enabling or Disabling IKE

Command	**crypto isakmp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	IKE is enabled by default. If you need to use IKE to negotiate IPSec SAs, this command is not required. If you do not use IKE to negotiate IPSec SAs, use the **no** form of this command to disable IKE.

Creating IKE Policy

Command	**crypto isakmp policy** *priority*
Parameter Description	*priority*: Indicates the priority.
Command Mode	Global configuration mode
Usage Guide	Use this command to specify parameters for negotiating IKE SAs. Run this command to enter the IKE policy configuration mode. In IKE policy configuration mode, you can set the following parameters: encryption(IKE policy): The default value is 56-bit DES-CBC. hash(IKE policy): The default value is SHA-1. authentication(IKE policy): The default value is RSA signature. group(IKE policy): The default value is 768-bit group. Diffie-Hellman lifetime(IKE policy): The default value is 86,400 seconds (1 day). If a parameter is not set, the default value of the parameter will be used. You can configure multiple IKE policies on the device. After the IKE negotiation starts, the device tries to find out the public policy configured at both ends, and the search starts from the policy with the highest priority on the remote peer.

Disabling the Transmission of Ruijie Vendor ID Information During IKE Negotiation

Command	**crypto isakmp vendorid disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Devices from some vendors cannot identify private vendor IDs during IKE negotiation, resulting in a negotiation failure. In this case, use this command to disable transmission of Ruijie vendor ID information.group(IKE policy): The default value is 768-bit group. Diffie-Hellman lifetime(IKE policy): The default value is 86,400 seconds (1 day). If a parameter is not set, the default value of the parameter will be used. You can configure multiple IKE policies on the device. After the IKE negotiation starts, the device tries to find out the public policy configured at both ends, and the search starts from the policy with the highest priority on the remote peer.

Specifying the First Peer that Initiates Negotiation in the Case of Multiple Peers.

Command	**crypto isakmp peer { bind | random }**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When 3G links are used, if multiple dialup addresses configured for a 3G card map to peers in the IPSec mapping set, enable the peer binding function to accelerate dialup. Otherwise, the device needs to try multiple times to find the correct peer. It takes a long time to establish a tunnel for the first time.

Configuring the Limit on the Number of IKE Negotiations.

Command	**crypto isakmp session limit** *numbers*
Parameter Description	*numbers*:Indicates the limit on the number of IKE negotiations.
Command Mode	Global configuration mode
Usage Guide	After the limit on the number of IKE negotiations is configured, the maximum number of clients that are allowed to initiate IKE negotiation cannot exceed this limit.

Disabling the NAT Traversal Function

Command	**crypto isakmp nat-traversal disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The protocols for implementing the NAT traversal function supported by devices of some vendors may be incompatible. In special cases, disable the NAT traversal function to implement device interworking.

Specifying the Encryption Algorithm for IKE Policies

Command	**encryption des | 3des | aes-128 | aes-192 | aes-256**
Parameter Description	des: Specifies the 56-bit DES-CBC as the encryption algorithm. 3des: Specifies the 168-bit 3DES-CBC as the encryption algorithm. aes-128: Specifies the AES with the 128-bit key as the encryption algorithm. aes-192: Specifies the AES with the 192-bit key as the encryption algorithm. aes-256: Specifies the AES with the 256-bit key as the encryption algorithm.
Command Mode	IKE policy configuration mode
Usage Guide	The data encryption algorithm specified by this command is used for encryption of IKE SA data. It differs from the encryption algorithm used by IPSec SAs. The DES encryption algorithm is used by default.

Specifying the Hash Algorithm for IKE Policies

Command	**hash** {**sha** | **md5**}
Parameter Description	sha: Specifies SHA-1 (HMAC variant) as the hash algorithm. md5: Specifies MD5 (HMAC variant) as the hash algorithm.
Command Mode	IKE policy configuration mode
Usage Guide	Use this command to specify the hash algorithm used in an IKE policy. The SHA algorithm is used by default.

Specifying the Authentication Method for IKE Policies

Command	**authentication** {**pre-share | rsa-sig | digital-email** }
Parameter	pre-share: Indicates a pre-shared key.

Description	rsa-sig: Indicates the digital certificate. digital-email: Indicates the digital email.
Command Mode	IKE policy configuration mode
Usage Guide	Currently, the authentication mode in an IKE negotiation policy uses the digital signature by default, which is the same as the authentication mode in Cisco devices. If you need to use pre-shared key authentication mode, you need to add an IKE policy, in which the pre-shared key authentication needs to be configured.

Specifying the ID of the Diffie-Hellman Group in IKE Policies

Command	**group** { **1** | **2** | **5** }
Parameter Description	**1**: Specifies 768-bit Diffie-Hellman group. **2**: Specifies 1024-bit Diffie-Hellman group. **5**: Specifies 1536-bit Diffie-Hellman group.
Command Mode	IKE policy configuration mode
Usage Guide	Use this command to specify the group applied in the IKE policy. By default, **group 1** is specified.

Specifying the lifetime of IKE SAs

Command	**lifetime** *seconds*
Parameter Description	*seconds*: Indicates the IKE tunnel timeout time.
Command Mode	IKE policy configuration mode
Usage Guide	Use this command to specify the lifetime of IKE SAs. When starting negotiation, IKE first reaches an agreement on session security parameters with the peer IKE. These consistent parameters will be referenced by IKE SAs on each peer and are retained on each peer till the IKE SA lifetime times out. A new SA must be negotiated prior to the expiration of the current SA. IPSec SAs are negotiated on the basis of IKE SAs. Therefore, a longer lifetime should be configured for IKE SAs to shorten the time required for negotiating IPSec SAs. However, the cracking probability is directly proportional to the lifetime. A longer lifetime indicates a higher cracking probability whereas a shorter lifetime indicates a lower cracking probability. Therefore, set a proper lifetime (for example, half a day) as required. The default value is **86,400** seconds.

Selecting Work Mode

Command	**set exchange-mode** { **main** | **aggressive** }
Parameter Description	main: Indicates the main mode. aggressive: Indicates the aggressive mode.
Command Mode	Encryption mapping configuration mode
Usage Guide	The IKE negotiation includes two phases: In Phase 1, a secure channel that passes authentication is established between two ISAKMP entities. The main mode or active mode can be adopted in this phase. In Phase 2, service SAs are negotiated.

	Select the required work mode in Phase 1 based on their advantages and disadvantages. The main mode is adopted by default. When IP addresses are not statically configured, the active mode is recommended.

Set Tunnel Auto-connection.

Command	**set autoup**
Parameter Description	*access-list-number*: indicates the ACL No. (100-199, 2000-2699, and 2900-3899). Encryption mapping entries use only IP extended ACLs.
Command Mode	Encryption mapping configuration mode
Usage Guide	Use this command to prevent packet loss caused by tunnel negotiation. Use this function in scenarios where data transmission is sensitive to tunnels and the tunnels need to be in the Up state at any time.

Specifying a Policy for Negotiating a Mapping Set

Command	**set isakmp-policy** *number*
Parameter Description	*Number*: i*ndicates the serial number of the specified policy for negotiation.*
Command Mode	Encryption mapping configuration mode
Usage Guide	In aggressive mode, the device in the branch sends the policy of the highest priority to the device in the headquarters for negotiation by default. Therefore, if the same device in the branch negotiates with multiple devices in the headquarters in aggressive mode, the policy of the highest priority on each device in the headquarters needs to be consistent with that on the device in the branch, which reduces device compatibility. Use this command to specify a policy for negotiating a mapping set. In this way, the policy of the highest priority on each device in the headquarters does not need to be consistent with that on the device in the branch. This command is effective only to static mapping sets and is unavailable to dynamic mapping sets.

Specifying the Local IP address in an Encryption Mapping Entry

Command	**set local** *ip-address*
Parameter Description	*ip-address*: *Indicates the local IP address.*
Command Mode	Encryption mapping configuration mode
Usage Guide	Use this command to set the local IP address used in the negotiation. The main address of the interface is used for negotiation when the IP address is not configured. The specified IP address is used for negotiation after configuration.

Setting the IPSec Pre-fragmentation Mode

Command	**set mtu** *length*
Parameter Description	*length*: *Indicates the size of a data packet fragment prior to encapsulation. The value range is from 512 to 1,500.*
Command	Encryption mapping configuration mode

Mode	
Usage Guide	Specify the pre-fragmentation mode for IPSec tunnel encapsulation.

Specifying a Remote Peer in an Encryption Mapping Entry

Command	**set peer** { *hostname* | *ip-address* }
Parameter Description	*ip-address*: *Indicates the IP address of the remote peer.* *hostname*: *Indicates the host name of the remote peer.*
Command Mode	Encryption mapping configuration mode
Usage Guide	A remote peer must be specified for an encryption mapping entry in use. When there are multiple certificate chains locally, specify the certificate chain according to each peer. If no local certificate chain is specified, the peer certificate chain (CA certificate) is used for authentication. When the peer certificate chain is not specified, the default certificate chain (CA certificate) is used for authentication.

Specifying Multiple ACEs to Use the Same Remote Peer in the Negotiation

Command	**set peer-identical**
Parameter Description	N/A
Command Mode	Encryption mapping configuration mode
Usage Guide	When multiple ACEs are configured in an ACL and multiple remote peers are configured, use this command to ensure that all ACEs use the same peer for negotiation.

Specifying the Remote Peer of a Higher Priority to Initiate Preemption.

Command	**set peer-preempt**
Parameter Description	N/A
Command Mode	Encryption mapping configuration mode
Usage Guide	Use the peer of a higher priority for negotiation when multiple remote peers are configured. Multiple remote peers can be configured for one encryption mapping set. A remote peer configured earlier has a priority higher than that of a remote peer configured later. The peer of a higher priority is used for negotiation. When the device switches to another peer for negotiation after a tunnel is interrupted, if the peer of a higher priority can initiate negotiation, the peer of the higher priority is used for negotiation and forwarding and the tunnel negotiation using the peer of a lower priority is interrupted. This command must be configured to implement the preceding functions.

Specifying the Diffie-Hellman group ID used in IPSec tunnel encapsulation.

Command	**set pfs** { **group1 | group2** }
Parameter Description	*group1*: Indicates the 768-bit group. *group2*: Indicates the 1024-bit group.
Command Mode	Encryption mapping configuration mode

Usage Guide	Specify the Diffie-Hellman group ID used in IPSec tunnel encapsulation.

Setting the Global Lifetime Used for IPSec SA Association in an Encryption Mapping Set.

Command	**set security-association lifetime** { **seconds** *seconds* | **kilobytes** *kilobytes*] }
Parameter Description	*seconds*:Indicates the SA timeout period in seconds. The value range is from 120 to 86400. *kilobytes*:Indicates the timeout communication amount of an SA in kilobytes. The value range is from 2,560 to 536,870,912.
Command Mode	Encryption mapping configuration mode
Usage Guide	This command is effective only to encryption mapping entries used for negotiation of IPSec SAs established via IKE and is unavailable to encryption mapping entries of SAs that are manually configured. By default, all IPSec SAs are negotiated based on the global lifetime. If a different lifetime is required for SA negotiation for a specific destination IP address, use this command to change the lifetime in the encryption mapping entry that uses this destination address for negotiation.

Enabling the Reverse Route Injection Function

Command	**reverse-route** [**remote-peer** *ip-address* | **no-peer**] [***distance***]
Parameter Description	*ip-address*: Specifies the next-hop address. *distance*: Specifies the next-hop distance. The value range is from 1 to 255.
Command Mode	Encryption mapping configuration mode
Usage Guide	no-peer is used to directly destine the route to the interface without specifying the next-hop for PPPoE etc.

(Optional) Configuring Local Identity

Command	**self-identity** { **address** | **trustpoint** *trustpoint* | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }
Parameter Description	self-identity: Indicates the local ID type and name. address: Indicates the local IP address. trustpoint: Specifies the local certificate. fqdn: Uses the full domain name. user-fqdn: Uses the email address.
Command Mode	Global configuration mode
Usage Guide	Set the identity for the negotiation initiated in active mode. You can use the domain name or address to specify the local identity.

(Optional) Configuring Automatic Identification of Work Mode

Command	**Crypto isakmp mode-detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Many vendors set foot in security products but the implementation methods of security products

	from different vendors are different. Two work modes are supported in Phase 1 of IKE negotiation. To ensure compatibility, use this command to complete negotiation in active mode when the IKE negotiation initiated by the peer cannot be completed.

Configuring Pre-shared Key

Command	**crypto isakmp key** { **0** | **7** } *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }
Parameter Description	address: Specifies the address that uses the key. hostname: Specifies the domain name that uses the key.
Command Mode	Global configuration mode
Usage Guide	In general, IKE uses a pre-shared key for negotiation. To enable IKE to successfully establish IKE SAs, you must use this command to configure the same pre-shared key on both communication peers. If the specified peer is a network segment, use **mask** to identify the subnet mask. When both **peer-address** and **Mask** are **0.0.0.0**, the default pre-shared key is used.

(Optional) Configuring DPD Detection

Command	**crypto isakmp keepalive** *seconds* [*retries*] [**on-demand** | **periodic**]
Parameter Description	*seconds*: Indicates the detection duration. *retries*: Indicates the detection interval. periodic: Indicates the interval mode. on-demand: Indicates the packet triggering mode.
Command Mode	Global configuration mode
Usage Guide	DPD detection is disabled by default. Extra overheads can be reduced in packet triggering mode. In periodic mode, the response is faster. Therefore, select a proper detection mode as required.

Setting IKE Negotiation Rate

Command	**crypto isakmp limit rate** *numbers*
Parameter Description	*numbers*: Indicates the rate limit.
Command Mode	Global configuration mode
Usage Guide	The rate limit function is enabled by default. The default rate limit is 1000. Change the value as required or run the **crypto isakmp limit disable** command to disable the rate limit function.

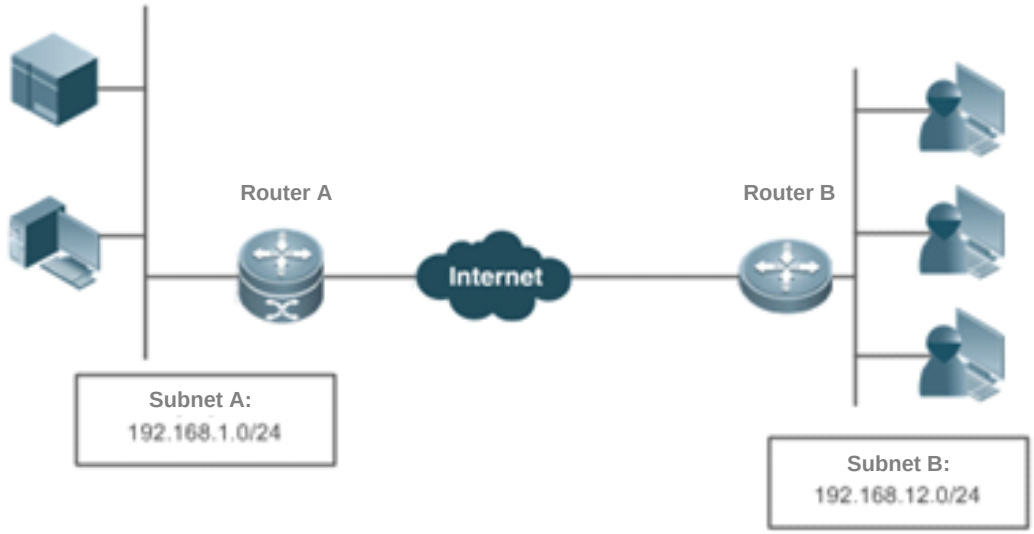
Setting the Port Switchover Time in IKE Negotiation

Command	**crypto isakmp port-repeat numbers**
Parameter Description	*Numbers*: Sets the port switchover period.
Command Mode	Global configuration mode
Usage Guide	The port switchover period is about 5 minutes by default, which can be modified based on actual conditions.

(Optional) Setting NAT Traversal Timeout Parameter

Command	**Crypto isakmp nat keepalive** *secs*
Parameter Description	*secs:* Indicates the interval for sending keepalive packets.
Command Mode	Global configuration mode
Usage Guide	The device complies with RFC3947 and uses the IPSEC NAT-T technology and UDP headers to resolve the NAT traversal problem. The keepalive mode is used for transmitting packets to prevent NAT connection timeout. Run the **crypto isakmp nat keepalive** command to specify the interval for sending keepalive messages. If the interval is not specified, the default value (5 minutes) is used.

Configuration Example

Scenario Figure 2-3	
	The IP data communication between two subnets needs to be protected. Ruijie Router A is used as a central gateway and connects to Subnet A. Ruijie Router B is used as a branch gateway and connects to Subnet B. The implementation requirements are as follows: ● The tunnel mode is used. ● The protection mode is ESP-DES-MD5 (providing encryption and authentication services). ● The IP address of the WAN interface on Router A is fixed to 202.1.1.2/24 and the WAN interface is connected to the Internet over a dedicated line. ● Router B connects to the Internet over PPPoE through the ADSL and the IP address of Router B is dynamically assigned by the ISP. ● The pre-shared key is used and the central router uses the host name to specify the pre-shared key. ● IKE is used to establish SAs.
Configuration Steps Router A	● An IPSec VPN tunnel is a point-to-point encryption tunnel. Devices at both ends of the tunnel encrypt and decrypt data via the negotiated key. IKE needs to be configured before an IPSec VPN tunnel is established. ● **Configuration on Router A:** # Define an IKE policy, in which the authentication method uses the pre-shared key and other

parameters use default values.

```
Hostname(config)#crypto isakmp policy 1
Hostname(isakmp-policy)#authentication pre-share
```

Configure the default pre-shared key. The IP address of the peer is dynamically assigned. Therefore, specify the host name to search for the pre-shared key.

```
Hostname(config)#crypto isakmp key 0 preword hostname www.google.com
```

Configure the automatic identification of the work mode on the central router.

```
Hostname(config)#crypto isakmp mode-detect
```

Define a transformation set.

```
Hostname(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac
```

Define dynamic encryption mapping.

```
Hostname(config)#crypto dynamic-map dymymap 5
Hostname(config-crypto-map)#set transform-set myset
Hostname(config-crypto-map)#match address 101
```

Add a dynamic encryption mapping set to the static encryption mapping set.

```
Hostname(config)#crypto map mymap 10 ipsec-isakmp dynamic  dymymap
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0
```

Apply the encryption mapping set to an interface.

```
Hostname(config)#interface serial 0
Hostname(config-if-serial 0)#ip address 202.1.1.2 255.255.255.0
Hostname(config-if-serial 0)#encapsulation ppp
Hostname(config-if-serial 0)#crypto map mymap
Hostname(config)#ip route 0.0.0.0 0.0.0.0  Serial0
```

Define an encryption access list to protect the IP communication between the subnet 192.168.1.0/24 and the subnet 192.168.12.0/24.

```
Hostname(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.12.0 0.0.0.255
```

- **Configuration on Router B:**

Enable IKE.

```
Hostname(config)#crypto isakmp enable
```

Configure the local identity.

```
Hostname(config)#self-identity fqdn www.google.com
```

Define an IKE policy, in which the authentication method uses the pre-shared key and other parameters use default values.

```
Hostname(config)#crypto isakmp policy 1
Hostname(isakmp-policy)#authentication pre-share
```

Configure a pre-shared key and transformation set.

```
Hostname(config)#crypto isakmp key 0 preword address 202.1.1.2
Hostname(config)#crypto ipsec transform-set myset    esp-des esp-md5-hmac
```

Define an encryption mapping set.

```
Hostname(config)#crypto map mymap 5 ipsec-isakmp
Hostname(config-crypto-map)#set peer 202.1.1.2
Hostname(config-crypto-map)#set exchange-mode aggressive
Hostname(config-crypto-map)#set transform-set myset
Hostname(config-crypto-map)#match address 101
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.12.1 255.255.255.0
Hostname(config)#interface MTGigabitEthernet 0/2
Hostname(config-if-MTGigabitEthernet 0/2)#no ip addrsss
Hostname(config-if-MTGigabitEthernet 0/2)#pppoe enable
Hostname(config-if-MTGigabitEthernet 0/2)#pppoe-client 1 dial-pool-number 1 dial-on-demand
```

Apply the encryption mapping set to an interface.

```
Hostname(config)#interface dialer 0
Hostname(config-if-dialer 0)#mtu 1488
Hostname(config-if-dialer 0)#ip address negotiate
Hostname(config-if-dialer 0)#encapsulation ppp
Hostname(config-if-dialer 0)#ppp pap sent-username xxx password xxx
Hostname(config-if-dialer 0)#crypto map mymap
Hostname(config-if-dialer 0)#dialer idle-timeout 2400
Hostname(config-if-dialer 0)#dialer pool 1
Hostname(config-if-dialer 0)#dialer-group 1
Hostname(config)#dialer-list protocol ip permit
Hostname(config)#ip route 0.0.0.0 0.0.0.0 Dialer0 permanent
```

Define an encryption access list to protect the IP communication between the subnet 192.168.12.0/24 and the subnet 192.168.1.0/24.

```
Hostname(config)#access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.1.0 0.0.0.255
```

2.5 Monitoring

Clearing

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

Description	Command
Clears IKE connections.	**clear crypto isakmp** [*connection-id*]

Displaying

Description	Command
Displays all IKE policy parameters.	**show crypto isakmp policy**
Displays all current IKE SAs.	**show crypto isakmp sa**

Debugging

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

Description	Command
Debugs IKE events.	**debug crypto isakmp**

1 Configuring PPPoE Client

1.1 Overview

PPPoE: Point-to-point Protocol Over Ethernet

Products support the PPPoE client on Ethernet interfaces, and are therefore able to connect to a host network by accessing a remote hub through a simple access device. The PPPoE protocol enables the PPPoE server to control each access client and perform relevant accounting.

- The PPPoE client is applicable in scenarios where Internet access is implemented through ADSL.

The following sections describe the PPPoE client only.

Protocols and Standards

- RFC2516: A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC1661: The Point-to-Point Protocol (PPP)

1.2 Applications

Application	Description
ADSL Scenario	In a scenario where Internet access is implemented through the Asymmetric Digital Subscriber Line (ADSL) technology, the device provides dialup and packet forwarding functions.

1.2.1 ADSL Scenario

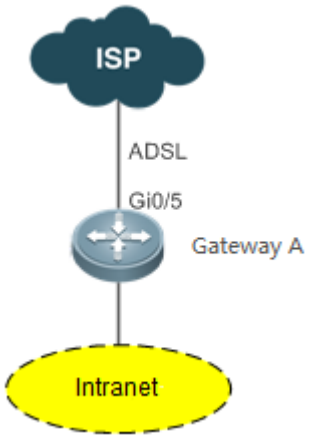
Scenario

In a scenario where Internet access is implemented through ADSL, the device provides dialup and packet forwarding functions.

The dialup networking scenario is illustrated with Figure 7-1 as an example.

- The dialup function is enabled on the device. The device connects to a remote Internet service provider (ISP) over an ADSL line, and obtains Internet access capability.
- Intranet PCs access the Internet through the device.

Figure 7-1



Corresponding Protocols

- Enable the dialup function on the device, and dial up to the Internet over the ADSL line.

1.3 Features

Basic Concepts

ISP

A network operator who provides users with Internet access service, information service, and value-added services (VASs).

ADSL

A line on which users dial up to the Internet.

Data Flow

A flow of packets only forwarded by the device.

Interested Flow

A specific type of packets defined by users during configuration, which can trigger the device to start dialup.

Overview

Feature	Description
Dialup to the Internet	In a scenario where Internet access is implemented through the Asymmetric Digital Subscriber Line (ADSL) technology, the device provides dialup and packet forwarding functions.

1.3.1 Dialup to the Internet

The device has Internet access capability after the dialup is complete; therefore, hosts in the intranet also have Internet access capability.

Working Principle

Dialup corresponds to the negotiation process, whereas Internet access corresponds to the packet forwarding process.

Negotiation can be further divided into three parts: protocol negotiation, protocol keepalive, and protocol termination.

↘ Protocol Negotiation

Protocol negotiation is divided into PPPoE negotiation and PPP negotiation.

During PPPoE negotiation, both parties confirm a unique peer, record the peer's MAC address, and establish a unique session ID.

During PPP negotiation, the server checks the client's authentication information. If the client passes the authentication, the server allocates an IP address to the client. If the client has already been configured with an IP address and the configured IP address meets the server's requirements, the server will agree to use this IP address as the IP address of the client.

After both protocols are up, the device has Internet access capability and prepares a Layer 2 (L2) header that is necessary for data packet encapsulation.

↘ Protocol Keepalive

After PPP is up, both parties periodically send LCP heartbeat packets to each other. If the party at one end does not receive any heartbeat response from the other party, it actively terminates the protocol.

↘ Protocol Termination

In certain cases, either party may actively terminate the protocol.

The initiating party sends a PPP termination packet to end the current PPP session, and then sends a PPPoE termination packet to end the current PPPoE session.

After receiving the PPP termination packet, the passive party returns an acknowledgement packet to agree to the termination of the PPP session; and after receiving the PPPoE termination packet, the passive party returns another acknowledgement packet to agree to the termination of the PPPoE session.

Once either party receives a PPPoE termination protocol, the PPP session and the PPPoE session will immediately terminate, even if it has not received any PPP termination protocol.

↘ Packet Forwarding

Packet sending process: When a data packet is routed to the dialer interface, the device encapsulates the data packet with the prepared L2 header information and ultimately sends the data packet from a physical port.

Packet receiving process: After a packet arrives at a physical port, the device marks the Layer 3 (L3) header position of the packet, executes the next service, and ultimately sends the packet to a host in the intranet.

Configuration

Configuring the Ethernet Interface

By default, the following functions are disabled and there is no corresponding default value.

Run the **pppoe enable** command to enable the PPPoE client function on the interface.

Run the **no pppoe enable** command to disable the PPPoE client function on the interface.

Run the **pppoe-client dial-pool-number** *pool-number* **no-ddr** command to bind the Ethernet interface to a specific logical dialer pool. The logical dialer pool provides automatic dialing and is always online.

Run the **no pppoe-client dial-pool-number** *pool-number* command to unbind the Ethernet interface from the specific logical dialer pool.

Run the **pppoe session mac-address** *H.H.H* command to configure the MAC address of a PPPoE session.

Configuring the Logical Interface

By default, the following functions are disabled.

Run the **interface dialer** *dialer-number* command to add a specific logical interface and enter the configuration mode of the logical interface.

Run the **no interface dialer** *dialer-number* command to delete the specific logical interface.

Run the **ip address negotiate** command to configure negotiation-based IP address acquisition.

Run the **no ip address negotiate** command to remove the configuration of negotiation-based IP address acquisition.

Run the **dialer pool** *number* command to associate a dialer pool, which corresponds to the dialer pool configured on the Ethernet interface.

Run the **no dialer pool** *number* command to remove the association with the dialer pool.

Run the **encapsulation ppp** command to configure the encapsulation protocol PPP. PPPoE is established on the basis of PPP.

Run the **no encapsulation** command to remove the encapsulation protocol configuration.

Run the **mtu** *1488* command to set the Maximum Transmit Unit (MTU) to 1488.

Run the **no mtu** command to remove the MTU configuration.

Run the **dialer-group** *dialer-group-number* command to associate a dialer triggering rule, which corresponds to the dialer-list.

Run the **no dialer-group** command to remove the configuration of the dialer triggering rule.

Run the **ppp chap hostname** *username* command to configure the user name for CHAP authentication.

Run the **no ppp chap hostname** command to remove the user name configuration for CHAP authentication.

Run the **ppp chap password** *password* command to configure the password for CHAP authentication.

Run the **no ppp chap password** command to remove the password configuration for CHAP authentication.

Run the **ppp pap sent-username** *username* **password** *password* command to configure the user name and password for PAH authentication.

Run the **no ppp pap sent-username** command to remove the user name and password configuration for PAH authentication.

Configuring Mandatory Global Parameters

By default, the following functions are disabled and shall be configured according to actual requirements. If other functional modules need to be used together, you also need to configure other global parameters.

Run the **dialer-list number protocol** *protocol-name* { **permit** | **deny** | **list** *access-list-number* } command to define a dialer triggering rule.

Run the **no dialer-list number** command to delete the configured dialer triggering rule.

Run the **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* [**permanent**] command to configure a route. If you specify the **permanent** option, the route will be always valid, even if the logical interface is within the enable-timeout period, in which case the logical interface will be down.

Run the **no ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* command to remove the route.

1.4 Configuration

Configuration	Description	
Configuring Basic Functions of the PPPoE Client	Global configuration mode	
	enable	Enables the PPPoE client function.
	pppoe-client dial-pool-number *number* { **dial-on-demand** | **no-ddr** }	Binds a logical dialer pool and specifies the dialing mode.
	pppoe session mac-address ***H.H.H***	Configures the MAC Address of the PPPoE Session
	interface-type interface-number	Adds a specific logical interface and enters the configuration mode of the logical interface.
	ip address { **negotiate** | *ip-addr subnet-mask* [**secondary**] }	Configures the IP address acquisition mode.
	dialer pool *number*	Associates a dialer pool.
	encapsulation ppp	Configures the encapsulation protocol PPP.
	mtu *1488*	Sets the MTU to 1488.
	dialer-group *dialer-group-number*	Associates a dialer triggering rule.
	ppp chap hostname *username*	Configures the user name for CHAP authentication.
	ppp chap password *password*	Configures the password for CHAP authentication.
	ppp pap sent-username *username* **password** *password*	Configures the user name and password for PAP authentication.
	ppp max-bad-auth *number*	Sets PPP authentication retry count.

Configuration	Description	
	dialer enable-timeout *seconds*	Configures the timeout period for the ASDL line.
	dialer hold-queue *packets* [**timeout** *seconds*]	Configures a hold queue on a DDR dialer interface.
	dialer idle-timeout *seconds*	Specifies the idle period for an ADSL line.
	dialer-list *dialer-group* **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }	Defines a dialer triggering rule.
	The configuration is optional.	
	ppp max-bad-auth	Run the command to specify the number of PPP authentication re-attempts.

1.4.1 Configuring Basic Functions of the PPPoE Client

Networking Requirements

- The device initiates PPPoE negotiation, and completes the negotiation process, protocol keepalive, and protocol termination.
- The device obtains Internet access capability after the negotiation is complete, and starts to forward a data flow which is routed to the dialer interface.

Notes

- After the kernel module is uninstalled, users can still perform configuration management but negotiation and data flow forwarding cannot be performed.

Configuration

↘ Enabling the PPPoE Client Function

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Enable the PPPoE client function.

↘ Binding a Logical Dialer Pool and Specifying the Dialing Mode

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Bind the Ethernet interface to a specific logical dialer pool and specify the dialer mode.

↘ Configuring the MAC Address of a PPPoE Session

- The configuration is mandatory.
- Perform this configuration on an Ethernet interface.

- Specify the MAC address of the PPPoE session for sub-interface dialing.

Adding a Specific Logical Interface and Entering the Configuration Mode of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in global configuration mode.
- Add a specific logical interface and enter its configuration mode.

Configuring the Way of Acquiring the IP Address of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the way of acquiring the IP address of the logical interface.

Associating a Dialer Pool

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Associate the logical interface with a specific dialer pool.

Configuring the Encapsulation Protocol

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the encapsulation protocol PPP on the logical interface.

Configuring the MTU of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Set the MTU of the logical interface to 1488.

Associating a Dialer Triggering Rule

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Associate a dialer triggering rule.

Configuring the User Name for CHAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the user name for CHAP authentication.

Configuring the Password for CHAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.

- Configure the password for CHAP authentication.

Configuring the User Name and Password for PAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the user name and password for PAP authentication.

Defining a Dialer Triggering Rule

- The configuration is mandatory.
- Perform this configuration in global configuration mode.
- Define a dialer triggering rule.

Configuring the Number of PPP Authentication Re-attempts

- The configuration is optional.
- Perform this configuration in the interface configuration mode.
- The number of PPP authentication re-attempts includes the first authentication. That is, if the number of PPP authentication re-attempts is set to 3, re-authentication can be performed twice after the first authentication fails. When the last authentication fails, the line is interrupted or reset.

Verification

- Check whether the dialer interface has acquired an IP address.
- Check whether a correct dialer interface route entry has been established on the device.

Related Commands

Enabling the PPPoE Client Function

Command	**enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	The interface on which the PPPoE client will be enabled must be a WAN Ethernet interface.

Binding a Logical Dialer Pool and Specifying the Dialing Mode

Command	**pppoe-client dial-pool-number** *number* { **dial-on-demand** | **no-ddr** }
Parameter Description	*number*: number of the dialer pool
Command Mode	Interface configuration mode
Configuration Usage	The PPPoE client function must be enabled on the interface first.

Configuring the MAC Address of the PPPoE Session

Command	**pppoe session mac-address** *H.H.H*
Parameter Description	*H.H.H*: MAC address
Command Mode	Interface configuration mode
Configuration Usage	The PPPoE client function must be enabled on the subinterface first.

Adding a Specific Logical Interface and Entering its Configuration Mode

Command	**interface dialer** *dialer-number*
Parameter Description	*dialer-number*: interface number
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Way of Acquiring the IP Address of the Logical Interface

Command	**ip address** { **negotiate** | *ip-addr subnet-mask* }
Parameter Description	*ip-addr*: manually configured IP address *subnet-mask*: manually configured subnet mask
Command Mode	Interface configuration mode
Configuration Usage	If you select **negotiate**, the IP address of the dialer interface will be acquired through negotiation. If you manually specify the IP address of the dialer interface, the peer's consent is required during negotiation for the device to work properly.

Associating a Dialer Pool

Command	**dialer pool** *number*
Parameter Description	*number*: number of the dialer pool
Command Mode	Interface configuration mode
Configuration Usage	An Ethernet interface will be selected from the dialer pool as the dialer interface to perform dialing.

Configuring the Encapsulation Protocol

Command	**encapsulation ppp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the MTU of the Logical Interface

Command	**mtu** *1488*
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	Because Internet access is implemented through the PPPoE protocol, the L2 header of a packet is longer than that of a common Ethernet packet.

Associating a Dialer Triggering Rule

Command	**dialer-group** *dialer-group-number*
Parameter Description	*dialer-group-number*: number of the dialer triggering rule
Command Mode	Interface configuration mode
Configuration Usage	If the DDR mode is specified, the device will be triggered to perform dialing only when a packet meeting the rule is routed to the dialer interface. If the no-DDR mode is specified, the configuration will not take effect on the device.

Configuring the User Name for CHAP Authentication

Command	**ppp chap hostname** *username*
Parameter Description	*username*: user name
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the Password for CHAP Authentication

Command	**ppp chap password** *password*
Parameter Description	*password*: password
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the User Name and Password for PAP Authentication

Command	**ppp pap sent-username** *username* **password** *password*
Parameter Description	*username*: user name *password*: password
Command Mode	Interface configuration mode
Configuration Usage	N/A

Defining a Dialer Triggering Rule

Command	**dialer-list number protocol** *protocol-name ip* { **permit** | **deny** | **list** *access-list-number* }
Parameter Description	*protocol-name*: protocol name *access-list-number*: ACL number
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Number of PPP Authentication Re-attempts

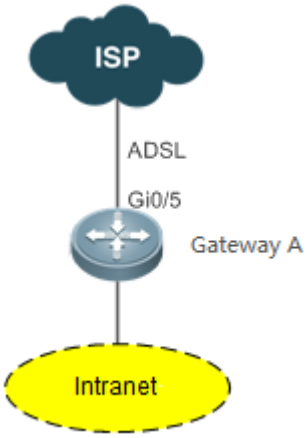
Command	**ppp max-bad-auth** *number*
Parameter Description	*number*: Indicates the Number of PPP authentication re-attempts, in the range from 1 to 255
Command Mode	Interface configuration mode
Usage Guide	N/A
	The following configuration example only describes configurations related to PPPoE clients.

The following configuration example describes configuration related to the PPPoE client only.

In the ADSL scenario, enable the PPPoE client function and access the Internet through an ADSL line.

Scenario

Figure 7-2



Configuration Steps	● Enable the PPPoE client function on the device, and add the interface Gi0/1 to the dialer pool.
	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if)# pppoe enable A(config-if)# pppoe-client dial-pool-number 1 dial-on-demand A(config-if)# exit A(config)# interface dialer 1 A(config-if)# ip address negotiate A(config-if)# mtu 1488 A(config-if)# encapsulation ppp A(config-if)# ip nat outside A(config-if)# dialer pool 1 A(config-if)# dialer-group 1 A(config-if)# ppp chap hostname pppoe A(config-if)# ppp chap password pppoe A(config-if)# ppp pap sent-username pppoe password pppoe A(config-if)# exit A(config)# access-list 1 permit any A(config)# dialer-list 1 protocol ip permit A(config)# ip nat inside source list 1 interface dialer 1 A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1 A(config)# end
Verification	Run the **show ip interface brief | in dialer** *1* command to check whether the dialer interface has acquired an IP address. Run the **show ip route** command to check whether a correct dialer interface route entry has been established. A# show ip interface brief | in dialer 1 dialer 1 49.1.1.127/32 YES UP

	A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is 0.0.0.0 to network 0.0.0.0 S* 0.0.0.0/0 is directly connected, dialer 1 C 10.10.3.0/24 is directly connected, GigabitEthernet 0/1 C 10.10.3.1/32 is local host. C 10.202.172.1/32 is directly connected, dialer 1 C 49.1.1.127/32 is local host.
Configuration Steps	Enable the PPPoE client multiple dial-up function on the device, and set up two dial-up links on Gi 0/1.
B	A# configure terminal A(config)# pppoe multi-dial enable A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# pppoe enable A(config-if-GigabitEthernet 0/1)# pppoe-client dial-pool-number 1 no-ddr A(config-if-GigabitEthernet 0/1)# pppoe-client dial-pool-number 2 no-ddr A(config-if-GigabitEthernet 0/1)#exit A(config)# interface dialer 1 A(config-if-dialer 1)# ip address negotiate A(config-if-dialer 1)# mtu 1488 A(config-if-dialer 1)# ip nat outside A(config-if-dialer 1)# dialer pool 1 A(config-if-dialer 1)# ppp chap hostname pppoe A(config-if-dialer 1)# ppp chap password pppoe A(config-if-dialer 1)# ppp pap sent-username pppoe password pppoe A(config-if-dialer 1)# exit A(config)# interface dialer 2 A(config-if-dialer 2)# ip address negotiate A(config-if-dialer 2)# mtu 1488 A(config-if-dialer 2)# ip nat outside A(config-if-dialer 2)# dialer pool 2 A(config-if-dialer 2)# ppp chap hostname pppoe1 A(config-if-dialer 2)# ppp chap password pppoe1

	A(config-if-dialer 2)# ppp pap sent-username pppoe1 password pppoe1 A(config-if-dialer 2)# exit A(config)# ip nat inside source list 1 interface dialer 1 A(config)# ip nat inside source list 1 interface dialer 2 A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1 A(config)# ip route 0.0.0.0 0.0.0.0 dialer 2 A(config)# end
Verification	Run the **show ip route** command to check whether a correct dialer interface routing entry has been created. A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is 0.0.0.0 to network 0.0.0.0 S* 0.0.0.0/0 is directly connected, dialer 1 S* 0.0.0.0/0 is directly connected, dialer 2 C 10.10.3.0/24 is directly connected, GigabitEthernet 0/0 C 10.10.3.1/32 is local host. C 10.202.172.1/32 is directly connected, dialer 1 C 10.202.172.2/32 is directly connected, dialer 2 C 49.1.1.127/32 is local host.

Common Errors

- The negotiation fails because the user name or password is incorrect.
- Intranet hosts cannot access the Internet because NAT configuration is incorrect.
- Intranet hosts cannot access the Internet because route configuration is incorrect.

1.5 Monitoring

Clearing

⚠ If you run the **clear pppoe tunnel** command while the device is operating, packet forwarding will be interrupted due to tunnel clearance.

Description	Command
Clears statistics about the DDR dialer interface.	**clear dialer** [*interface-type interface-number*]
Clears the tunnel.	**clear pppoe tunnel**

Displaying

Description	Command
Displays information about the DDR dialer.	**show dialer** [**interface** *interface-* type *interface-*number] [**maps**] [**pools**]
Displays PPPoE status information.	**show pppoe** { **ref** | **session** | **tunnel** }

Debugging

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

Description	Command
Enables the DDR debugging switch.	**debug dialer** { **pkt** | **mlp**|**callback**|**event** }
Enables the PPP negotiation debugging switch.	**debug ppp** [**authentication** | **error** | **event** | **negotiation** | **packet**]
Enables the PPPoE negotiation debugging switch.	**debug pppoe** [**datas** | **errors** | **events** | **packets**]